Algebra 2

Karl-Heinz Fieseler

Uppsala 2015

Contents

1 Översikt

Vi börjar med en repetition av heltalsaritmetiken: Med hjälp av de första nya begreppen *ideal* och *principalideal* bevisar vi aritmetikens fundamentalsats Th.2.1. Sedan diskuterar vi restklassaritmetiken, där man fixerar ett naturligt tal $n > 1$, också kallat *moduln*, och identifierar två heltal om deras differens är delbar genom n.

I båda fall finns det två räkneoperationer, addition och multiplikation: Det leder till begreppet *ring*, Def. 4.1, en mängd R utrustad med två binära operationer som liknar addition och multiplikation av heltal. Som exempel hittar vi $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ och restklassringarna $\mathbb{Z}_n$.

Särskilt roliga är ringar, där man också har en division, de kallas för *kroppar*: $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ och restklassringarna $\mathbb{Z}_p$ med ett primtal p som modul är

exempel.

Nu händer det att man vill lösa en ekvation

$$x^n + \lambda_{n-1}x^{n-1} + ... + \lambda_1 x + \lambda_0 = 0$$

med koefficienter $\lambda_i \in K$. Att hitta en explicit formel för en lösning x går bara för $n \leq 4$, och det försöker vi inte heller. Inte ens finns det alltid en lösnig i själva kroppen K: T.ex. har

$$x^2 + 1 = 0$$

ingen lösning i $\mathbb{R}$. Vi beskriver ett sätt (Th.8.11) hur man, given ovanstående ekvation över kroppen K, kan hitta en större kropp $E \supset K$, sådant att

$$x^n + \lambda_{n-1}x^{n-1} + ... + \lambda_1 x + \lambda_0 = (x - \alpha_1) \cdot ... \cdot (x - \alpha_n)$$

med $\alpha_1, ..., \alpha_n \in E$. I synnerhet är alltså $\alpha_1, ..., \alpha_n \in E$ lösningarna till vår ekvation i kroppen $E \supset K$. Om $K = \mathbb{Q}, \mathbb{R}$, så kan vi ta $E = \mathbb{C}$ enligt algebrans fundamentalsats (Th.12.3). Men om vi i stället ta $K = \mathbb{Z}_p$, får vi någonting nytt: För varje primtal p och naturligt tal n konstruerar vi en kropp

$$\mathbb{F}_{p^n} \supset \mathbb{Z}_p$$

med p^n element (Th.10.2). Ett viktigt verktyg visar sig vara polynomringen $K[X]$ vars element är "formella summor" (polynom)

$$\beta_m X^m + \beta_{m-1}X^{m-1} + ... + \beta_1 X + \beta_0$$

med koefficienter $\beta_i \in K$. De nya kropparna är faktorringar av polynomringen $K[X]$.

I polynomringen $K[X]$ gäller aritmetikens fundamentalsats likaså som i heltalsringen $\mathbb{Z}$ (Th.7.17), och i avsnitt 11 diskuterar vi en tredje ring, där det är så, ringen

$$\mathbb{Z}[i] = \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C}$$

av alla *Gaußiska heltal*, dvs. komplexa tal med heltal som real- och imaginärdel.

Det sista avsnittet ingår inte i kursen: Där berättar vi hur man kommer fram från $\mathbb{N}$ till $\mathbb{C}$, i synnerhet, hur de reella talen kan skapas från $\mathbb{Q}$, och presenterar ett enkelt bevis till algebrans fundamentalsats Th.12.3.

2 Heltalsaritmetik

Vi påminner om *aritmetikens fundamentalsats*:

Theorem 2.1. *Låt $n \in \mathbb{N}_{>1}$. Om*

$$n = p_1 \cdot .... \cdot p_r = q_1 \cdot .... \cdot q_s$$

med primtal $p_1 \leq p_2 \leq ... \leq p_r, q_1 \leq q_2 \leq ... \leq q_s$, så gäller $s = r$ och $p_i = q_i$ för $i = 1, ..., r = s$.

Det resultat som ligger bakom är följande egenskap för primtal:

Theorem 2.2. *För ett primtal $p \in \mathbb{N}$ gäller*

$$p|ab \Longrightarrow p|a \vee p|b.$$

För att visa detta behöver vi lite kunskap om den största gemensamma delaren av två heltal a, b:

Definition 2.3. För heltal $a, b \in \mathbb{Z}$ inte samtidigt $= 0$ definieras deras största gemensamma delare genom

$$\text{sgd}(a, b) := \max\{q \in \mathbb{N}_{>0}; q|a, q|b\}.$$

Nästa sats visas med Euklides' algoritm, men vi ska härleda den här på ett mer kortfattat (och mindre konstruktivt) sätt:

Theorem 2.4. *Den största gemensamma delaren av heltal $a, b \in \mathbb{Z}$ med $(a, b) \neq (0, 0)$ kan skrivas som en linjärkombination i a och b med heltalskoefficienter, dvs.*

$$\text{sgd}(a, b) = ra + sb$$

med lämpliga heltal $r, s \in \mathbb{Z}$. I synnerhet gäller

$$q|a, q|b \Longrightarrow q|\text{sgd}(a, b).$$

Bevis till Th.2.2. Vi antar att p inte delar a och visar $p|b$. Eftersom primtalet p bara har p och 1 som positiva delare, har vi

$$1 = \text{sgd}(p, a) = rp + sa$$

med lämpliga heltal $r, s \in \mathbb{Z}$. Men sedan är

$$b = brp + s(ab)$$

delbart med p. □

För att visa Th. 2.4 tittar vi på mängden

$$\mathbb{Z}a + \mathbb{Z}b := \{ka + \ell b; k, \ell \in \mathbb{Z}\}$$

av alla linjärkombinationer med heltalskoefficienter i a och b. Den utgör ett "ideal":

Definition 2.5. En icke-tom delmängd $\mathfrak{a} \subset \mathbb{Z}$ kallas ett

1. *ideal* om den är sluten både
   (a) m.a.p. additionen:
   $$\mathfrak{a} + \mathfrak{a} \subset \mathfrak{a},$$
   eller med andra ord: $x, y \in \mathfrak{a} \Longrightarrow x + y \in \mathfrak{a}$,
   (b) och m.a.p. godtycklig heltalsmultiplikation:
   $$\mathbb{Z} \cdot \mathfrak{a} \subset \mathfrak{a},$$
   eller med andra ord: $k \in \mathbb{Z}, x \in \mathfrak{a} \Longrightarrow kx \in \mathfrak{a}$.
2. *principalideal* (eller *huvudideal*) om
   $$\mathfrak{a} = \mathbb{Z}n$$
   för något heltal $n \in \mathbb{Z}$.

Remark 2.6.
1. $0 \in \mathfrak{a}$ för varje ideal $\mathfrak{a} \subset \mathbb{Z}$: Om $a \in \mathfrak{a}$, så också $-a = (-1)a \in \mathfrak{a}$ och $0 = a + (-a) \in \mathfrak{a}$.
2. En icke-tom additivt sluten delmängd $\mathfrak{a} \subset \mathbb{Z}$ är ett ideal omm den ligger symmetriskt m.a.p. origo, dvs. omm
   $$-\mathfrak{a} = \mathfrak{a}.$$

Theorem 2.7. *Varje ideal $\mathfrak{a} \subset \mathbb{Z}$ är ett principalideal:*

$$\mathfrak{a} = \mathbb{Z}n$$

med ett entydigt bestämt naturligt tal $n \in \mathbb{N}$.

Proof. Om $\mathfrak{a} = \{0\}$, så ta $n = 0$. Om inte, så har vi

$$\mathfrak{a}_{>0} := \{a \in \mathfrak{a}; a > 0\} \neq \emptyset$$

pga. $\mathfrak{a} = -\mathfrak{a}$ och tar

$$n := \min \mathfrak{a}_{>0}.$$

Eftersom $n \in \mathfrak{a}$ och $\mathfrak{a}$ är sluten m.a.p. godtycklig heltalsmultiplikation, får vi $\mathbb{Z}n \subset \mathfrak{a}$. Ta nu ett tal $a \in \mathfrak{a}$ och använd divisionsalgoritmen

$$a = qn + r,\ 0 \leq r < n.$$

Sedan har vi två möjligheter:

1. $r = 0$ och således $a \in \mathbb{Z}n$, eller
2. $r = a - qn \in \mathfrak{a}_{>0}$. Men då följer $r \geq \min \mathfrak{a}_{>0} = n$, en motsägelse.

□

Till sist avslutas beviset till Teorem 2.4 med

Proposition 2.8. *Om*

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}n,$$

där $(a, b) \neq (0, 0)$ *och* $n \in \mathbb{N}$*, så gäller*

$$n = \text{sgd}(a, b).$$

Proof. Vi har $q := \text{sgd}(a, b) \geq n$, eftersom n delar både a och b. Å andra sidan delar q i sin tur såväl a som b, således också talet $n = ra + sb$. Men

$$q|n \wedge q \geq n \Longrightarrow q = n.$$

□

Det återstår att hitta

$$\text{sgd}(a, b) = \min(\mathbb{Z}a + \mathbb{Z}b)_{>0}.$$

Men den här beskrivningen har man inte mycket glädje av: Man kan ju inte pröva sig igenom alla $k, \ell \in \mathbb{Z}$ med $ka + \ell b > 0$. Här hjälper nu Euklides' algoritm med vilken vi kan reducera talen a och b. Den bygger på följande enkel, men nyttig anmärkning:

Remark 2.9. Om $a = qn + r$, så gäller

$$\mathbb{Z}a + \mathbb{Z}b = \mathbb{Z}b + \mathbb{Z}r.$$

Euklides' algoritm är nu en iteration av detta steg:

1. Vi får anta $a \geq b \geq 0$.
2. Om $a = b$ eller $b = 0$, så blir $\mathrm{sgd}(a, b) = a$.
3. Om däremot $a > b > 0$, skriver vi $a = qb + r$ och ovanstående anmärkning ger oss
$$\mathrm{sgd}(a, b) = \mathrm{sgd}(b, r).$$
4. Och sedan börjar hela proceduren på nytt med paret (b, r) i stället för (a, b). Eftersom $a > b > r \geq 0$, hamnar vi någon gång i situationen, där en division går jämnt ut. Då är det sista positiva talet i följden $a, b, r, ...$ den största gemensamma delaren till a och b.

3 Restklassaritmetik

Låt $n \in \mathbb{N}_{>1}$ vara ett heltal > 1.

Definition 3.1. Två heltal $a, b \in \mathbb{Z}$ kallas kongruent modulo n, skrivet som:

$$a \equiv b \mod (n)$$

eller

$$a \overset{n}{\equiv} b,$$

omm n delar differensen $b - a$.

Remark 3.2.
1. $.. \overset{n}{\equiv} ..$ är en ekvivalensrelation.
2. Ekvivalensklassen
$$R_n(a) := \{b \in \mathbb{Z}; b \overset{n}{\equiv} a\}$$
till ett heltal $a \in \mathbb{Z}$ uppfyller
$$R_n(a) = a + \mathbb{Z}n := \{a + kn; k \in \mathbb{Z}\}.$$

3. Vi påminner om att
$$R_n(a) = R_n(b) \Longleftrightarrow a \overset{n}{\equiv} b.$$

4. För $0 \leq r < n$ består $R_n(r)$ av alla de heltal som lämnar resten r efter division med n, dvs. $a = qn + r$. Därför kallas ekvivalensklasserna också för restklasser (eller n-restklasser). Vi får således en partition
$$\mathbb{Z} = \bigcup_{i=0}^{n-1} R_n(i).$$

5. Mängden av alla n-restklasser skrivs så här:
$$\mathbb{Z}_n := \{R_n(i); i = 0, ..., n-1\}.$$

Aritmetiska operationer för n-restklasser: Vi vill nu införa en addition och en multiplikation
$$\mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$$
för restklasser. Vi börjar med den elementvisa additionen och multiplikationen av delmängder $A, B \subset \mathbb{Z}$, nämligen
$$A + B := \{a + b; a \in A, b \in B\}$$
och
$$AB := \{ab; a \in A, b \in B\}.$$

Proposition 3.3. *1.* $R_n(a) + R_n(b) = R_n(a + b)$,

2. $R_n(a) \cdot R_n(b) \subset R_n(ab)$, *där*

3. $R_n(ab) = R_n(a) \cdot R_n(b) + \mathbb{Z}n$.

Proof. Vi tittar på summan resp. produkten av två godtyckliga tal $a + kn \in R_n(a)$ och $b + \ell n \in R_n(b)$ och ser att
$$(a + kn) + (b + \ell n) = (a + b) + (k + \ell)n$$
och
$$(a + kn)(b + \ell n) = ab + (kb + \ell a + k\ell n)n.$$
Eftersom alla element i den elementvisa produkten ligger i samma n-restklass $R_n(ab)$, kan vi helt enkelt "fylla på" med $\mathbb{Z}n$ och erhåller hela n-restklassen $R_n(ab)$. □

Remark 3.4. I själva verket är den elementvisa produkten av n-restklasser inte nödvändigtvis igen en n-restklass, t.ex. har vi

$$R_n(0) \cdot R_n(0) = \mathbb{Z}n \cdot \mathbb{Z}n = \mathbb{Z}n^2 = R_{n^2}(0).$$

Som addition tar vi nu

$$\alpha : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, (R_n(a), R_n(b)) \mapsto R_n(a+b) = R_n(a) + R_n(b),$$

den elementvisa summan, medan vid multiplikationen måste vi "fylla på" den elementvisa produkten:

$$\mu : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n, (R_n(a), R_n(b)) \mapsto R_n(ab) = R_n(a) \cdot R_n(b) + \mathbb{Z}n.$$

En enklare notation: För att underlätta livet inför vi en enklare notation, där "moduln" n är underförstådd: Vi skriver

$$\overline{a} := R_n(a) = a + \mathbb{Z}n,$$

sådant att

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}.$$

Sedan tar additionen och multiplikationen av n-restklasser följande enkel form:

$$\overline{a} + \overline{b} = \overline{a+b}$$

och

$$\overline{a} \cdot \overline{b} = \overline{ab}.$$

Observera: Från och med nu använder vi konventionen, att i strecknotationen $.. \cdot ..$ betecknar inte den elementvisa produkten av två n-restklasser, utan den entydiga n-restklassen den är inkluderad i, dvs:

$$\overline{a} \cdot \overline{b} = R_n(a) \cdot R_n(b) + \mathbb{Z}n = \overline{ab}.$$

Exempel: Låt oss till sist ange några additions- och multiplikationstabeller:

1. Additionstabellen för $\mathbb{Z}_2$ blir

$$\begin{array}{c|cc} + & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{1} \\ \overline{1} & \overline{1} & \overline{0} \end{array} \quad ,$$

   medan multiplikationstabellen ser så här ut

$$\begin{array}{c|cc} \cdot & \overline{0} & \overline{1} \\ \hline \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} \end{array} \quad .$$

2. Additionstabellen för $\mathbb{Z}_3$ blir

$$\begin{array}{c|ccc} + & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} \\ \overline{1} & \overline{1} & \overline{2} & \overline{0} \\ \overline{2} & \overline{2} & \overline{0} & \overline{1} \end{array} \quad ,$$

   medan multiplikationstabellen ser så här ut

$$\begin{array}{c|ccc} \cdot & \overline{0} & \overline{1} & \overline{2} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} \\ \overline{2} & \overline{0} & \overline{2} & \overline{1} \end{array} \quad .$$

3. Additionstabellen för $\mathbb{Z}_4$ blir

$$\begin{array}{c|cccc} + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\ \overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\ \overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \end{array} \quad ,$$

   medan multiplikationstabellen ser så här ut

$$\begin{array}{c|cccc} \cdot & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \hline \overline{0} & \overline{0} & \overline{0} & \overline{0} & \overline{0} \\ \overline{1} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\ \overline{2} & \overline{0} & \overline{2} & \overline{0} & \overline{2} \\ \overline{3} & \overline{0} & \overline{3} & \overline{2} & \overline{1} \end{array} \quad .$$

Vi avslutar avsnittet med en liten

Räkneövning: Vi vill beräkna a^{162} för $a = \overline{3} \in \mathbb{Z}_{121}$. Receptet är följande: Vi löser upp hela räkningen i en rad steg bestående antingen

1. av en kvadrering $b \mapsto b^2$ eller
2. en multiplikation $c \mapsto ca$.

Man börjar ovanifrån och skriver ner de exponenter $n \in \mathbb{N}$, för vilka man måste beräkna potenser a^n. Efter det beräknar man potenserna nedifrån. Idén är helt enkelt att

1. för $n = 2k$ vi har $a^n = b^2$ med $b = a^k$, eller
2. för $n = 2k + 1$ vi har $a^n = b^2 a$ med $b = a^k$,

där man redan har kommit fram till b.

n	162	81	80	40	20	10	5	4	2	1
$\overline{3}^n$	$\overline{9}$	$\overline{3}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$\overline{1}$	$-\overline{40}$	$\overline{9}$	$\overline{3}$

.

Vi ska se senare att $a^{110} = \overline{1}$ för alla $a = \overline{\ell}$, där ℓ inte är delbar med 11. Det skulle ha gett

$$a^{162} = a^{110+52} = a^{110}a^{52} = a^{52}$$

och sedan har vi tabellen

n	52	26	13	12	6	3	2	1
$\overline{3}^n$	$\overline{9}$	$\overline{3}$	$\overline{27}$	$\overline{9}$	$\overline{3}$	$\overline{27}$	$\overline{9}$	$\overline{3}$

.

4 Ringar

Vi har diskuterat restklassaritmetik för att förbereda nästa definition:

Definition 4.1. En *ring* är en trippel (R, α, μ) bestående av en mängd R och två avbildningar

$$\alpha : R \times R \longrightarrow R, (a, b) \mapsto a + b := \alpha(a, b) \quad ,$$

"additionen", och

$$\mu : R \times R \longrightarrow R, (a, b) \mapsto ab := \mu(a, b) \quad ,$$

"multiplikationen", sådant att

1. den associativa lagen

$$(a+b)+c = a+(b+c),\ (ab)c = a(bc)$$

gäller för både addition och multiplikation,

2. den kommutativa lagen

$$a+b = b+a$$

gäller för additionen,

3. de "distributiva" lagarna

$$a(b+c) = ab+ac\ ,\ (a+b)c = ac+bc$$

gäller för alla $a, b, c \in R$,

4. det finns ett element $0 \in R$, sådant att

$$a+0 = 0$$

för alla $a \in R$,

5. det finns ett element $1 \in R$, sådant att

$$1 \cdot a = a = a \cdot 1\ ,\quad \forall a \in R\ ,$$

6. för varje $a \in R$ finns det ett element $b \in R$ med

$$a+b = 0.$$

En ring kallas *kommutativ* om den kommutativa lagen också gäller för multiplikationen:

$$ba = ab.$$

Example 4.2. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$ är kommutativa ringar.

OBS: Alla ringar i de här anteckningarna förutsätts stillatigande vara komutativa ringar!

Remark 4.3. 1. Elementen $0, 1$ är entydiga och kallas för ringens nolla och ringens etta. Om nämligen $\tilde{0}$ resp. $\tilde{1}$ skulle ha samma egenskap, fick vi

$$\tilde{0} = \tilde{0} + 0 = 0 + \tilde{0} = 0$$

och

$$\tilde{1} = \tilde{1} \cdot 1 = 1.$$

2. Elementet $b \in R$ med $a + b = 0$ är entydig: Om $\tilde{b}$ är ett element med samma egenskap, så har vi

$$b = 0 + b = (a + \tilde{b}) + b = (\tilde{b} + a) + b = \tilde{b} + (a + b) = \tilde{b} + 0 = \tilde{b}.$$

Elementet b skrivs vanligtvis som $-a$.

3. Nollan uppfyller

$$0 \cdot a = 0 = a \cdot 0$$

för alla $a \in R$: Vi har $a = 1 \cdot a = (1 + 0)a = a + 0 \cdot a$ och adderar $-a$ till båda led.

4. På samma sätt följer

$$(-1)a = a(-1) = -a$$

från $0 = 0 \cdot a = (1 + (-1))a = a + (-1)a$.

5. Vi har $1 = 0$ omm $R = \{0\}$. Vi kallar R då för nollringen.

Vi ska nu diskutera olika slags element i en ring R: I fall implikationen

$$b = 0 \Longrightarrow ab = 0$$

kan omvändas:

$$ab = 0 \Longrightarrow b = 0$$

har elementet $a \in R$ äran att få ett särskilt namn:

Definition 4.4. 1. Ett element $a \in R$ i en kommutativ ring R kallas för en *icke-nolldelare* omm $ab = 0 \Longrightarrow b = 0$.

2. En icke-trivial ring (inte nollringen), där alla element $a \neq 0$ är icke-nolldelare kallas för ett *integritetsområde* (integral domain).

Example 4.5. 1. Ringarna $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ är integritetsområden.

2. Icke-nolldelare kan strykas i en ekvation: $ax = ay \Longrightarrow x = y$.

3. En n-restklass $\overline{a} \in \mathbb{Z}_n$ är en icke-nolldelare omm $\text{sgd}(a, n) = 1$. Vi har

$$\overline{a} \cdot \overline{b} = \overline{ab} = \overline{0} \Longleftrightarrow \exists k \in \mathbb{Z} : \ ab = kn.$$

Om $\text{sgd}(a, n) = 1$ innebär detta att $n|b$, dvs. $\overline{b} = \overline{0}$. Å andra sidan om $\text{sgd}(a, n) = d > 1$, har vi $n = n_0 d$ och $n|an_0$, dvs.

$$\overline{a} \cdot \overline{n}_0 = \overline{0},$$

fast $\overline{n}_0 \neq \overline{0}$.

4. Restklassringen $\mathbb{Z}_n$ är ett integritetsområde omm $n = p$ är ett primtal, eftersom ett naturligt tal är ett primtal omm alla tal $k, 1 \leq k < n$ är relativ prima till n.

Definition 4.6. 1. Ett element $a \in R$ i en icke-trivial ring R kallas *invertibart* eller en *enhet* omm det finns ett element $b \in R$ med $ab = ba = 1$.

2. Mängden

$$R^* := \{a \in R; \exists b \in R : \ ab = ba = 1\}$$

av alla inverterbara element kallas för ringens *enhetsgrupp*.

3. En kommutativ ring med $R^* = R \setminus \{0\}$ kallas en *kropp* (*field*).

Example 4.7. 1. Talet b med $ab = ba = 1$ är entydigt bestämt, vi skriver $a^{-1} := b$.

2. Enhetsgruppen är sluten m.a.p. multiplikation och inversion. I själva verket gäller

$$(ab)^{-1} = b^{-1}a^{-1}, (a^{-1})^{-1} = a.$$

3. Enheter är icke-nolldelare: Om $a \in R^*$ och $ab = 0$, hittar vi $0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$.

4. I en ändlig (kommutativ) ring är icke-nolldelare redan enheter, eftersom multiplikationen med a, avbildningen $\mu_a : R \longrightarrow R, x \mapsto ax$, är injektiv och en injektiv självavbildning av en ändlig mängd är också surjektiv. I synnerhet finns det $b \in R$ med $\mu_a(b) = 1$.

5. $\mathbb{Z}^* = \{\pm 1\}$.

6. $\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n;\ \text{sgd}(a,n) = 1\}$.

7. $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ och $\mathbb{Z}_p$ med ett primtal p är kroppar.

8. Vi beräknar $\overline{r} = \overline{70}^{-1} \in \mathbb{Z}_{101}$:, dvs. vi måste lösa kongruensen $70r \equiv 1$ mod (101). Vi letar efter $r, s \in \mathbb{Z}$ med

   (a) $70r + 101s = 1$

   (b) $70x + 31s = 1$

   (c) $8x + 31y = 1$

   (d) $8z - y = 1$

   Vi reducerar 101 mod 70 och byter samtidigt r till $x = r + s$, sedan reducerar vi 70 mod 31 och byter ut s mot y osv. Till sist tar vi $z = 0, y = -1$. Det ger $x = 4, s = -9, r = 13$. Således: $\overline{70}^{-1} = \overline{13} \in \mathbb{Z}_{101}$.

Kongruenser och ekvationer i någon restklassring: En ekvation

$$\alpha\xi = \beta$$

för $\xi = \overline{x} \in \mathbb{Z}_n$ skrivs klassiskt som

$$ax \equiv b \mod (n),$$

där $x \in \mathbb{Z}, \alpha = \overline{a}, \beta = \overline{b}$. Lösningsmängden av kongruensen är en union av restklasser

$$\bigcup_{\nu=1}^{r} \xi_\nu \subset \mathbb{Z},$$

där $\xi_\nu, \nu = 1, ..., r$, är lösningarna till $\alpha\xi = \beta$. Vi har:

Example 4.8. Ekvationen $\overline{4}\cdot\xi = \overline{0}$ i $\mathbb{Z}_6$ har lösningarna $\overline{0}, \overline{3}$, medan lösningarna till kongruensen $4x \equiv 0 \mod (6)$ är elemeten i $\mathbb{Z}6 \cup (3 + \mathbb{Z}6) = \mathbb{Z}3$.

Proposition 4.9. *Kongruensen*

$$ax \equiv b \mod (n)$$

är lösbar omm $\text{sgd}(a,n)|b$. *Närmare bestämt:*

1. *Om* $\text{sgd}(a, n) = 1$*, är lösningsmängden restklassen*

$$\overline{a}^{-1} \cdot \overline{b} \in \mathbb{Z}_n.$$

2. *Om* $d = \text{sgd}(a, n)$ *och* $a = a_0 d, n = n_0 d, b = b_0 d$*, så gäller*

$$ax \equiv b \mod (n) \Longleftrightarrow a_0 x \equiv b_0 \mod (n_0).$$

Således, om $x_0 \in \mathbb{Z}$ *är en lösning, så är*

$$R_{n_0}(x_0) = \bigcup_{k=0}^{d-1} R_n(x_0 + kn_0)$$

hela lösningsmängden.

Proof. Lösbarhet är ekvivalent med $b \in \mathbb{Z}a - \mathbb{Z}n = \mathbb{Z} \cdot \text{sgd}(a, n)$. □

Example 4.10. Vi löser kongruensen $251x \equiv 125 \mod (521)$ med samma metod som $70x \equiv 1 \mod (101)$.

1. $251x - 521y = 125$
2. $251z - 19y = 125$
3. $4z - 19t = -8$.

If we take $z = -2$, we obtain $y = -33$ and $x = -68$. So $x \equiv -68 \mod (521)$ is the solution.

Definition 4.11. Funktionen $\varphi : \mathbb{N}_{>0} \longrightarrow \mathbb{N}$ definierad som

$$\varphi(n) := \begin{cases} 1 & , \text{ om } n = 1 \\ |\mathbb{Z}_n^*| & , \text{ om } n \geq 2 \end{cases}$$

kallas för *Eulers* φ*-funktion.*

Lemma 4.12. *För en primtalspotens* $n = p^k, k \geq 1$*, får vi:*

$$\varphi(p^k) = p^{k-1}(p - 1) \ .$$

Proof. Komplementet till $\mathbb{Z}_{p^k}^*$ utgörs av nolldelarna

$$\overline{0}, \overline{p}, \overline{2p}, ..., \overline{(p^{k-1}-1)p}.$$

Således

$$|\mathbb{Z}_{p^k}^*| = |\mathbb{Z}_{p^k}| - \text{antalet nolldelare} = p^k - p^{k-1} = p^{k-1}(p-1).$$

□

Theorem 4.13 (Lagrange)**.** *Låt R vara en kommutativ ring. Om enhetsgruppen R^* är ändlig, så gäller*

$$a^{|R^*|} = 1$$

för alla $a \in R^*$.

Proof. Avbildningen $\mu_a : R^* \longrightarrow R^*, x \mapsto ax$, är bijektiv, således

$$\prod_{x \in R^*} x = \prod_{x \in R^*} \mu_a(x) = \prod_{x \in R^*} (ax) = a^{|R^*|} \prod_{x \in R^*} x.$$

Eftersom $\prod_{x \in R^*} x \in R^*$ är en icke-nolldelare, följer $1 = a^{|R^*|}$. □

Corollary 4.14 (Fermat's lilla sats)**.** *För en restklass $\overline{a} \in \mathbb{Z}_n^*$ har vi*

$$\overline{a}^{\varphi(n)} = \overline{1}.$$

Definition 4.15. Ett element

1. $e \in R$ kallas för *idempotent* omm $e^2 = e$.
2. $u \in R$ kallas för *nilpotent* omm det finns $n \in \mathbb{N}_{>0}$ med $u^n = 0$.

Example 4.16.

1. Elementen $0, 1 \in R$ är idempotenta. Restklasserna $\overline{3}, \overline{4} \in \mathbb{Z}_6$ är idempotenta.
2. Om $e \in R$ är idempotent, så är det $1 - e$ likaså.
3. I ett integritetsområde är $0, 1$ de enda idempotenta, eftersom $0 = e^2 - e = e(1-e)$ innebär $e = 0$ eller $e = 1$.
4. En restklass $\xi \in \mathbb{Z}_{p^k}$ är nilpotent omm den inte är en enhet.

5 Homomorfismer

För att förstå relationen mellan olika slags ringar behövs det "*ringhomomorfismer*":

Definition 5.1. Låt R, S vara ringar. En avbildning $\varphi : R \longrightarrow S$ kallas en *ringhomomorfism* omm

1. $$\varphi(a+b) = \varphi(a) + \varphi(b) \ , \ \varphi(ab) = \varphi(a)\varphi(b)$$
   för alla $a, b \in R$,

2. $$\varphi(1) = 1 \ ,$$
   där 1 betecknar ettan i respektive ring R och S.

Den kallas en *ringisomorfism* omm den ytterligare är bijektiv, och R är *isomorf* med S, skrivet som: $R \cong S$, omm det finns en ring isomorfism $\varphi : R \longrightarrow S$.

Remark 5.2. 1. För en ringhomomorfism $\varphi : R \longrightarrow S$ gäller

$$\varphi(0) = 0, \varphi(-a) = -\varphi(a)$$

pga. $\varphi(a) = \varphi(a+0) = \varphi(a) + \varphi(0)$ och $0 = \varphi(0) = \varphi(a + (-a)) = \varphi(a) + \varphi(-a)$.

2. Villkoret $\varphi(1) = 1$ är alltid uppfyllt om $\varphi(1) \neq 0$ och S är ett integritetsområde, eftersom idempotenta element $\neq 1$ är nolldelare.

Example 5.3. 1. För varje ring R finns precis en ringhomomorfism

$$\chi : \mathbb{Z} \longrightarrow R.$$

Nödvändigtvis har vi

$$\chi(n) = \begin{cases} \overbrace{1 + ... + 1}^{n\times} & , \ \text{om } n > 0 \\ 0 & , \ \text{om } n = 0 \\ \underbrace{(-1) + ... + (-1)}_{m\times} & , \ \text{om } n = -m < 0 \end{cases} .$$

Att det är en ringhomomorfism, följer från distributiva lagen. Vanligtvis skriver man inte $\chi(n) \in R$, utan bara

$$n := \chi(n),$$

men man skulle inte glömma, att $n = 0$ kan gälla i R fast det inte är fallet i $\mathbb{Z}$. Till exempel ta $R = \mathbb{Z}_n$!

2. För $m|n$ definierar

$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_m, R_n(a) \mapsto R_m(a) = R_n(a) + \mathbb{Z}m$$

en ringhomomorfism.

3. Komplexa konjugationen

$$\mathbb{C} \longrightarrow \mathbb{C}, z \mapsto \overline{z},$$

är en ringisomorfism.

Definition 5.4. Kärnan till en ringhomomorfism $\varphi : R \longrightarrow S$ är mängden

$$\ker(\varphi) := \varphi^{-1}(0) = \{x \in R; \varphi(x) = 0\}.$$

Remark 5.5. En ringhomomorfism $\varphi : R \longrightarrow S$ är injektiv omm $\ker(\varphi) = \{0\}$. Villkoret är uppenbarligen nödvändigt pga. $\varphi(0) = 0$, men det är också tillräckligt: Om $\varphi(x) = \varphi(y)$, så följer $\varphi(x - y) = \varphi(x) - \varphi(y) = 0$, i.e. $x - y \in \ker(\varphi) = \{0\}$ och således $x - y = 0$, dvs. $y = x$.

Kärnan utgör ett ideal:

Definition 5.6. En icke-tom delmängd $\mathfrak{a} \subset R$ av en kommutativ ring kallas ett

1. *ideal* om den är sluten både
   (a) m.a.p. additionen:
   $$\mathfrak{a} + \mathfrak{a} \subset \mathfrak{a},$$
   eller med andra ord: $x, y \in \mathfrak{a} \Longrightarrow x + y \in \mathfrak{a}$,
   (b) och m.a.p. multiplikation med ett godtyckligt element i R:
   $$R \cdot \mathfrak{a} \subset \mathfrak{a},$$
   eller med andra ord: $a \in R, x \in \mathfrak{a} \Longrightarrow ax \in \mathfrak{a}$.

2. *principalideal* (eller *huvudideal*) om

$$\mathfrak{a} = Rb$$

för något element $b \in R$.

Ett integritetsområde, där varje ideal är ett principalideal, kallas ett principalidealområde (PID=principal ideal domain).

Remark 5.7. 1. $\mathfrak{a} = \{0\}$ kallas nollidealet, $\mathfrak{a} = R$ enhetsidealet.

2. En kommutativ ring R är en kropp, omm noll- och enhetsidealet är de enda idealen.

3. En ringhomomorfism $\varphi : K \longrightarrow R$ från en kropp till en icke-trivial ring är alltid injektiv: Pga. $\varphi(1) = 1$, gäller $\ker(\varphi) \neq K$, således $\ker(\varphi) = \{0\}$.

Definition 5.8. Låt R vara en ring och $\chi : \mathbb{Z} \longrightarrow R$ den naturliga ringhomomorfismen. **Karakteristiken** $\mathrm{char}(R) \in \mathbb{N}$ av ringen R definieras som det naturliga tal $n \in \mathbb{N}$, sådant att

$$\ker(\chi) = \chi^{-1}(0) = \mathbb{Z}n \quad .$$

Med andra ord: Antingen $\mathrm{char}(R) = 0$ - i så fall är $\chi : \mathbb{Z} \longrightarrow R$ injektiv - eller

$$\mathrm{char}(R) = \min\{k \in \mathbb{N}_{>0}; k = 0 \text{ i } R\}.$$

Remark 5.9. För ett integritetsområde R är $\mathrm{char}(R) = 0$ eller ett primtal $\mathrm{char}(R) = p$.

Example 5.10. För en kropp K av $\mathrm{char}(K) = p > 0$ definieras *Frobeniushomomorfismen* som

$$\sigma = \sigma_K : K \longrightarrow K, x \mapsto x^p.$$

Uppenbarligen gäller $(xy)^p = x^p y^p$ och $1^p = 1$, men också

$$(x+y)^p = x^p + \sum_{k=1}^{p-1} \binom{p}{k} x^k y^{p-k} + y^p = x^p + y^p,$$

eftersom binomialkoefficienterna

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} \in \mathbb{N}$$

är delbara med p för $k = 1, ..., p-1$ - primtalet p ingår ju i täljaren, men inte i nämnaren - och således

$$\binom{p}{k} = 0 \in K,\ 1 \leq k \leq p-1.$$

Den är uppenbarligen injektiv, och även surjektiv om K är ändlig. I så fall pratar man om Frobeniusautomorfismen. Men tyvärr - för $K = \mathbb{Z}_p$ har vi $x^p = x$ enligt Lagrange, dvs. $\sigma_{\mathbb{Z}_p} = \mathrm{id}_{\mathbb{Z}_p}$. Så det verkar inte särskilt intressant. I själva verket spelar Frobeniushomomorfismen en central roll i teorin om kroppar av karaktäristik $p > 0$, och den är lika med identiteten bara för $K = \mathbb{Z}_p$.

Definition 5.11. Låt $R_1, ..., R_s$ vara ringar. Den direkta produkten $R_1 \times .... \times R_s$ är den kartesiska produkten av mängderna $R_1, ..., R_s$ tillsammans med den komponentvisa additionen och multiplikationen.

Theorem 5.12 (Kinesiska restsatsen)**.** *Låt $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ vara primtalsfaktoriseringen av det naturliga talet $n \in \mathbb{N}_{>1}$. Sedan är*

$$\psi : \mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}, \overline{a} \mapsto (a + \mathbb{Z}p_1^{k_1}, ..., a + \mathbb{Z}p_r^{k_r})$$

en ringisomorfism.

Proof. Eftersom "start"- och målringen har samma antal element, räcker det att visa att ψ är injektiv, m.a.o. att $\ker(\psi) = \{0\}$. Men $\psi(\overline{a}) = 0$ innebär $p_i^{k_i} | a$ för $i = 1, ..., r$, och detta ger $n|a$ resp. $\overline{a} = \overline{0}$. □

Corollary 5.13. *Låt $n = p_1^{k_1} \cdot ... \cdot p_r^{k_r}$ vara primtalsfaktoriseringen. Sedan*

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot ... \cdot \varphi(p_r^{k_r})$$

Proof. Kinesiska isomorfismen

$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}$$

inducerar en bijektion

$$\mathbb{Z}_n^* \longrightarrow \mathbb{Z}_{p_1^{k_1}}^* \times ... \times \mathbb{Z}_{p_r^{k_r}}^*.$$

□

Remark 5.14. För att invertera kinesiska isomorfismen letar vi efter inversa bilderna $\xi_i \in \mathbb{Z}_n$ till enhetsvektorerna $e_i \in \mathbb{Z}_{p_1^{k_1}} \times ... \times \mathbb{Z}_{p_r^{k_r}}$. Om vi har lyckats med den saken, så gäller

$$\psi^{-1}(\overline{a}_1, ..., \overline{a}_r) = a_1\xi_1 + ... + a_r\xi_r.$$

För att hitta elementen $\xi_i \in \mathbb{Z}_n$ tar vi $n_i := np_i^{-k_i} \in \mathbb{N}$ och löser kongruenserna

$$n_i x \equiv 1 \mod (p_i^{k_i})$$

med, säg, $x = \ell_i \in \mathbb{Z}$. Sedan blir

$$\xi_i = \overline{\ell_i n_i} \in \mathbb{Z}_n.$$

Om talen är små kan man förstås pröva sig igenom alla tal $\ell n_i, 0 \leq \ell < p_i^{k_i}$.

Example 5.15. Låt $n = 84 = 2^2 \cdot 3 \cdot 7$. Sedan får vi $n_1 = 21, n_2 = 28, n_3 = 12$ och $\ell_1 = 1, \ell_2 = 1, \ell_3 = 3$ och således $\xi_1 = \overline{21}, \xi_2 = \overline{28}, \xi_3 = \overline{36}$.

Public key cryptography, RSA-kryptering: (Rivest, Shamir, Adleman)

Situationen är följande: Det finns en mottagare, som får budskap från många sändare, men de vill inte att deras budskap läses av de andra sändare. Då kan mottagaren dela ut en offentlig nyckel till kryptering åt alla sändare, medan kunskapen om den nyckeln inte är tillräcklig för dechiffrering. För den behöver man någon information till. Så här kan det fungera:

1. Budskap motsvarar restklasser $\alpha \in \mathbb{Z}_n$ för något fast tal $n \gg 0$.

2. Den offentligt givna nyckeln för krypteringen: Ett tal $e \in \mathbb{N}$, som levereras av mottagaren, samma åt alla sändare.

3. Kryptering sker med potensavbildningen:

$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \alpha \mapsto \alpha^e.$$

4. Vad mottagaren har gjort: Han har tagit fram olika primtal p, q och valt $n = pq$ samt $e \in \mathbb{N}$, sådant att $\text{sgd}(e, \varphi(n)) = 1$, där $\varphi(n) = (p-1)(q-1)$. Talen p, q är hemliga, och eftersom faktorisering av stora tal är problematiskt, går det praktiskt taget inte att hitta p, q utgående från själva moduln n.

5. Mottagaren dechiffrerar med potensavbildningen

$$\mathbb{Z}_n \longrightarrow \mathbb{Z}_n, \beta \mapsto \beta^d,$$

där exponenten d uppfyller.

$$\alpha = (\alpha^e)^d = \alpha^{ed}, \quad \forall \alpha \in \mathbb{Z}_n.$$

6. Exponenten d väljs sådant att

$$ed \equiv 1 \mod (p-1)(q-1).$$

Här behövs faktoriseringen $n = pq$.

7. Om $\ell \equiv 1 \mod \varphi(n)$, så gäller

$$\alpha^\ell = \alpha$$

för alla $\alpha \in \mathbb{Z}_n$.

Proof of 7). Pga. $\mathbb{Z}_n \cong \mathbb{Z}_p \times \mathbb{Z}_q, \alpha \mapsto (\gamma, \delta)$, räcker det att visa

$$\gamma^\ell = \gamma, \delta^\ell = \delta.$$

Låt $\ell = 1 + m(p-1)(q-1)$. Vi får anta $\gamma \neq 0$ och får då

$$\gamma^\ell = \gamma \cdot (\gamma^{p-1})^{m(q-1)} = \gamma \cdot \overline{1}^{m(q-1)} = \gamma.$$

På samma sätt för δ. □

6 Bråkräkning

Låt R vara ett integritetsområde. På den kartesiska produkten $R \times (R \setminus \{0\})$ definierar vi ekvivalensrelationen $\sim$ på följande sätt

$$(a, s) \sim (b, t) :\Longleftrightarrow at = bs \ .$$

Symmetri och reflexivitet är klara, anta nu $(a, s) \sim (b, t) \sim (c, u)$. Det innebär $at = bs$ och $bu = ct$. Multiplikation med u resp. s leder till $atu =$

$bsu = cts$ resp. $au = cs$, eftersom R inte har nolldelare $\neq 0$. Således $(a, s) \sim (c, u)$. Mängden

$$Q(R) := R \times (R \setminus \{0\})/\sim$$

av dess ekvivalensklasser utgör en kropp, ringen R's *kvotkropp*. Beteckna med

$$\frac{a}{s} := [(a, s)] \in Q(R)$$

ekvivalensklassen av paret (a, s). Vi kollar att bråkräkningsreglerna ger väldefinierade ringoperationer: Additionen och multiplikationen fungerar så här

$$\frac{a}{s} + \frac{b}{t} := \frac{at + bs}{st} \ , \ \frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}.$$

Example 6.1. $Q(\mathbb{Z}) = \mathbb{Q}$.

Definition 6.2. Låt R, S vara (kommutativa) ringar. Om

$$R \ \subset \ S,$$

$$\text{sådant att} \quad 1_R \ = \ 1_S$$

och ringoperationerna i R är inskränkingarna på R av ringoperationerna i den större ringen S säger vi att

1. R är en *delring* till S,
2. S är en *ringutvidgning* till R.

En *kroppsutvidgning* är en ringutvidgning, där både R och S är kroppar. På samma sätt använder vi ordet *delkropp*.

Example 6.3.

1. Heltalsringen $\mathbb{Z}$ och restklassringerna $\mathbb{Z}_n$ har bara sig själv som delringar.
2. Kroppen $\mathbb{Q}$ har bara sig själv som delkropp, däremot många delringar, t.ex. $\mathbb{Z}$.
3. Låt $\chi : \mathbb{Z} \longrightarrow S$ vara den naturliga ringhomomorfismen. $R := \chi(\mathbb{Z}) \subset S$ är då den minsta delringen till S. Vi anmärker att $\chi(\mathbb{Z}) \cong \mathbb{Z}$ för $\text{char}(S) = 0$ och $\chi(\mathbb{Z}) \cong \mathbb{Z}_n$ för $\text{char}(S) = n$.

4. Låt R vara ett integritetsområde. Avbildningen $\iota : R \mapsto Q(R), a \mapsto \frac{a}{1}$, är uppenbarligen en injektiv ring homomorfism. Således kan R uppfattas som *delring* till $Q(R)$.

5. $\mathbb{Q} \subset \mathbb{R}, \mathbb{R} \subset \mathbb{C}$ är delkroppar.

6. $\mathbb{R} \times \{0\} \subset \mathbb{R} \times \mathbb{R}$ är inte någon delring.

Remark 6.4. Delringar och ideal: Skillnaden mellan ett ideal $\mathfrak{a} \subset S$ och en delring $R \subset S$ är följande:

1. En delring $R \subset S$ skulle vara multiplikativt sluten $R \cdot R \subset R$, medan för ett ideal krävs mer: $S \cdot \mathfrak{a} \subset \mathfrak{a}$.

2. För ett ideal $\mathfrak{a}$ krävs inte $1 \in \mathfrak{a}$. I själva verket, om det gäller, handlar det redan om enhetsidealet $\mathfrak{a} = S$.

Definition 6.5. Varje kropp K har en minsta delkropp $P(K)$, dess *primkropp*. Nämligen,

1. om $\mathrm{char}(K) = 0$, så är

$$P(K) = \{ab^{-1}; a, b \in \chi(\mathbb{Z}), b \neq 0\} \ \cong \mathbb{Q};$$

2. om $\mathrm{char}(K) = p$, så är

$$P(K) = \chi(\mathbb{Z}) \cong \mathbb{Z}_p$$

med den naturliga ringhomomorfismen $\chi : \mathbb{Z} \longrightarrow K$.

7 Polynomringen

Definition 7.1. Ett polynom med koefficienter i den kommutativa ringen R (eller över R) är ett "formellt uttryck"

$$f = \sum_{\nu=0}^{n} a_\nu X^\nu, \ a_0, ..., a_n \in R,$$

som kan användas för att definiera en funktion

$$f_S : S \longrightarrow S, x \mapsto f(x) := \sum_{\nu=0}^{n} a_\nu x^\nu.$$

för varje ring $S \supset R$. Mängden av alla polynom betecknas

$$R[X] := \left\{ \sum_{\nu=0}^{n} a_\nu X^\nu ; a_0, ..., a_n \in R, n \in \mathbb{N} \right\}.$$

Man kan alltså tänka sig X som ett slags variabel, men man bestämmer sig inte från början, var den skulle "variera".

Example 7.2. 1. f_R är inskränkningen av f_S till $R \subset S$, m.a.o. att gå upp i diagrammet

$$\begin{array}{ccc} S & \xrightarrow{f_S} & S \\ \cup & & \cup \\ R & \xrightarrow{f_R} & R \end{array}$$

från vänstra hörnet R och sedan följa pilen f_S leder till samma resultat som att först följa pilen f_R och sedan gå upp.

2. Ovanstående situation är egentligen ganska vanlig: Tänk på situationen $R = \mathbb{Z}, S = \mathbb{R}$. Ett polynom $f \in \mathbb{Z}[X]$ används både för att definiera funktionen

$$f_{\mathbb{Z}} : \mathbb{Z} \longrightarrow \mathbb{Z}$$

och funktionen

$$f_{\mathbb{R}} : \mathbb{R} \longrightarrow \mathbb{R}.$$

3. Ta $R = \mathbb{Z}_p, f = X^p - X$. Vi har

$$f_{\mathbb{Z}_p} = 0$$

pga. Lagrange's sats, men

$$f_K \neq 0$$

om $K \supsetneq \mathbb{Z}_p$ är en kroppsutvidgning, se Ex.7.5.

Remark 7.3. Polynom "bestäms av sina koefficienter", dvs.

$$f = \sum_{\nu=0}^{n} a_\nu X^\nu = 0 \Longleftrightarrow a_0 = ... = a_n = 0,$$

de adderas och multipliceras på det sedvanliga sättet. Mängden $R[X]$ blir således en kommutativ ring.

Givet ett polynom $f \in K[X]$ letar man ofta efter nollställen $a \in K$ till f. Om man har lyckats hitta ett nollställe $a \in K$, kan man reducera problemet så här:

Proposition 7.4. *Låt K vara en kropp och $a \in K$. Om $f(a) = 0$, kan vi skriva*

$$f = (X - a)g$$

med ett polynom $g \in K[X]$. I synnerhet, om $a_1, ..., a_r \in K$ är parvis olika nollställen till f kan vi faktorisera

$$f = (X - a_1) \cdot ... \cdot (X - a_r) \cdot h.$$

Example 7.5. För $f = X^p - X \in \mathbb{Z}_p[X]$ är varje $\alpha \in \mathbb{Z}_p$ ett nollställe. Sedan följer

$$X^p - X = \prod_{\alpha \in \mathbb{Z}_p} (X - \alpha),$$

eftersom $h = 1$ pga. att båda polynom är normerade av samma grad. I synnerhet gäller $f(x) \neq 0$ för alla $x \in K \setminus \mathbb{Z}_p$ för varje kroppsutvidgning $K \supset \mathbb{Z}_p$ - vi har ju $x - \alpha \neq 0$ för alla $\alpha \in \mathbb{Z}_p$ och K är ett integritetsområde.

Proof. Vi skriver

$$f = f((X - a) + a) = \sum_{\nu=1}^{n} c_\nu (X - a)^\nu = (X - a)g,$$

med $g = \sum_{\nu=1}^{n} c_\nu (X - a)^{\nu-1}$ – vi har ju $c_0 = f(a) = 0$. □

Definition 7.6. Ett nollställe $a \in K$ till polynomet $f \in K[X]$ kallas enkelt, om $g(a) \neq 0$.

Man kan kolla om ett nollställe är enkelt eller ej med hjälp av den "formella derivatan":

Definition 7.7. Låt K vara en kropp. Den *formella derivatan* $f' \in K[X]$ av ett polynom $f = \sum_{\nu=0}^{n} a_\nu X^\nu \in K[X]$ är polynomet

$$f' := \sum_{\nu=1}^{n} \nu a_\nu X^{\nu-1} \in K[X].$$

Remark 7.8. 1. $(f+g)' = f' + g', (fg)' = f'g + fg'$. Leibnizregeln visas först för monom $f = aX^m, g = bX^n$ och sedan utnyttjar man att båda led är additiva i f och g.

2. Om $\mathrm{char}(K) = 0$ har vi $f' = 0 \Longleftrightarrow f = a_0 \in K$.

3. Om $\mathrm{char}(K) = p$ har vi $f' = 0 \Longleftrightarrow f = h(X^p)$ med ett polynom $h \in K[X]$.

Proposition 7.9. *Låt $a \in K$ vara ett nollställe till $f \in K[X] \setminus K$. Sedan är a ett enkelt nollställe, dvs. $f = (X-a)g$ med $g(a) \neq 0$, omm $f'(a) \neq 0$.*

Example 7.10. Om $\mathrm{char}(K) = p$ och $q = p^n$, så har $f = X^q - X \in K[X]$ bara enkla nollställen pga. $f' = -1$.

Proof. Vi har

$$f' = g + (X-a)g'$$

och således

$$f'(a) = g(a).$$

□

Vi sammanställer nu några grundläggande egenskaper av polynomringar. Vi behöver gradfunktionen:

Definition 7.11. Låt R vara en ring. Gradfunktionen

$$\mathrm{grad} : R[X] \longrightarrow \mathbb{N} \cup \{-\infty\}$$

definieras för $f \in R[X]$ genom

$$\mathrm{grad}(f) := \begin{cases} n & , \quad \text{if } f = \sum_{\nu=0}^{n} a_\nu X^\nu, a_n \neq 0 \\ -\infty & , \quad \text{if } f = 0 \end{cases} .$$

Remark 7.12. 1. Man har

$$\mathrm{grad}(f+g) \leq \max(\mathrm{grad}(f), \mathrm{grad}(g)) \ , \ \mathrm{grad}(fg) \leq \mathrm{grad}(f) + \mathrm{grad}(g)$$

samt

$$\mathrm{grad}(fg) = \mathrm{grad}(f) + \mathrm{grad}(g)$$

om ett av polynomen f, g har en ickenolldelare som ledande koefficient, i synnerhet om R är ett inegritetsområde.

2. Polynomringen $R[X]$ över ett integritetsområde är igen ett integritetsområde.

3. För ett integritetsområde gäller

$$R[X]^* = R^*,$$

så $R[X]$ är inte en kropp.

4. Ett polynom $f \in R[X]$ över ett integritetsområde R her högst grad$f$ nollställen.

Polynomringen $K[X]$ över en kropp K beter sig i många avseenden som heltalsringen $\mathbb{Z}$. I skolan lär man sig:

Theorem 7.13 (**Divisionsalgoritm för polynom**). *Låt $g \in R[X], g \neq 0$, vara ett polynom vars ledande koefficient är en enhet. Varje polynom $f \in R[X]$ skrivs som*

$$f = qg + r$$

med entydigt bestämda polynom $q, r \in R[X], \text{grad}(r) < n = \text{grad}(g)$.

Proof. Entydighet: Låt $f = qg + r = \tilde{q}g + \tilde{r}$. Sedan:

$$(q - \tilde{q})g = (\tilde{r} - r) \ .$$

Polynomet på högra ledet har grad $< n$, medan för $q - \tilde{q} \neq 0$ vänstra ledet har minst grad n (eftersom g är normerat). Således $q = \tilde{q}$ och då förstås också $r = \tilde{r}$.
Existens: Vi använder induktion följande deg(f): Om deg$(f) < n$ tar vi $q = 0$ och $r = f$.
Om deg$(f) =: m \geq n$, kanske $f = b_m X^m + ... + b_0$, betraktar vi polynomet $\tilde{f} := f - b_m X^{m-n} g$. Eftersom det har grad $<$ deg(f), ger induktionshypotesen $\tilde{q}, \tilde{r}$ med

$$\tilde{f} = \tilde{q}g + \tilde{r}$$

och deg$(\tilde{r}) < n$. Slutligen ta $q := \tilde{q} + b_m X^{m-n}, r := \tilde{r}$. □

Som följdsats får vi:

Proposition 7.14. *Polynomringen $K[X]$ över en kropp K är ett principalidealområde: För ett icke-trivialt ideal $\mathfrak{a} \subset K[X]$ har vi*

$$\mathfrak{a} = K[X]f,$$

där $f \in K[X]$ är ett polynom av minsta grad i $\mathfrak{a} \setminus \{0\}$. Om vi förutsätter f vara normerat, är f entydigt bestämt.

Bevis av Prop. 7.14. Låt $\mathfrak{a} \subset K[T]$ vara ett ideal. Om $\mathfrak{a} \neq \{0\}$, kan vi välja ett polynom polynom $f \in \mathfrak{a} \setminus \{0\}$ av minsta grad, och efterrsom K är en kropp, kan vi anta att f är normerat. Sedan har vi $\mathfrak{a} = (f)$. Inklusionen "$\supset$" är självklart.
"$\subset$": Ta ett polynom $h \in \mathfrak{a}$. Divisionsalgoritmen 7.13 ger $h = qf + r$, var $\deg(r) < \deg(f)$. Men då, pga. $r = h - qf \in \mathfrak{a}$, nödvändigtvis $r = 0$ enligt val av f. Således $h = qf \in K[X]f$. □

Till sist blir det primfaktoriseringens tur:

Definition 7.15. Låt K vara en kropp. Ett polynom $f \in K[X] \setminus K$ kallas *irreducibelt*, om det inte kan faktoriseras

$$f = gh$$

med icke-konstanta polynom $g, h \in K[X]$. Man säger också att f är irreducibelt *över* K.

Example 7.16.

1. Ett kvadratiskt eller kubiskt polynom $f \in K[X]$ är irreducibelt omm f inte har något nollställe i K, eftersom i en eventuell faktorisering måste en av faktorerna vara linjär.

2. Polynomet $X^2 + 1 \in \mathbb{R}[X]$ är irreducibelt, men inte

$$X^2 + 1 = (X - i)(X + i) \in \mathbb{C}[X].$$

3. De enda normerade irreducibla polynomen $f \in \mathbb{C}[X]$ är de linjära polynomen $f = X - a, a \in \mathbb{C}$, pga. algebrans fundamentalsats Th.12.3.

4. Polynomet $X^3 - 2 \in \mathbb{Q}[X]$ är irreducibelt, eftersom det saknar rationella nollställen.

5. Alla rationella nollställen till ett polynom $f = X^n + \sum_{\nu=0}^{n-1} a_\nu X^\nu \in \mathbb{Z}[X]$ är heltal, i själva verket är de delare till den konstanta termen $a_0 \in \mathbb{Z}$. Om nämligen $f(\frac{p}{q}) = 0$ med $\mathrm{sgd}(p, q) = 0, q > 0$, så har vi

$$p^n = -q \left(\sum_{\nu=0}^{n-1} a_\nu p^\nu \cdot q^{n-\nu-1} \right),$$

men $q|p^n$ innebär $q = 1$. Och $a_0 = p\left(-p^{n-1} - \sum_{\nu=1}^{n-1} a_\nu p^{\nu-1}\right)$ är delbart med p.

6. Polynomet $X^3 - 3X + 1 \in \mathbb{Q}[X]$ är irreducibelt, eftersom det inte har några rationella nollställen: De vore ju redan heltal enligt förenående punkt och delare till konstanta termen 1. Men $f(\pm 1) \neq 0$.

Theorem 7.17 (Aritmetikens fundamentalsats för polynom)**.** *Låt K vara en kropp.*

1. *För ett irreducibelt polynom $p \in K[X]$ gäller*

$$p|gh \Longrightarrow p|g \vee p|h.$$

för $g, h \in K[X]$.

2. *Varje normerat polynom $f \in K[X]$ kan faktoriseras*

$$f = p_1 \cdot .... \cdot p_r,$$

som produkt av irreducibla normerade polynom. Faktorerna är entydiga så när som på omkastning.

Proof. Gör det själv, det är samma sak som i fallet av heltalsringen $\mathbb{Z}$. □

8 Faktorringar

Om ett polynom $f \in K[X] \setminus K$ inte har något nollställe i själva kroppen K, så vore det ganska fint, om man kunde konstruera en större kropp $L \supset K$ - en *kroppsutvidgning* till K - , där f har ett nollställe: Den första idén är av en helt formell natur: Man tar en ny kopia $K[Y]$ av polynomringen $K[X]$

och identifierar två polynom i Y om deras differens är delbar genom $f(Y)$ - här är

$$f(Y) = \sum_{\nu=0}^{n} a_\nu Y^\nu \text{ för } f = \sum_{\nu=0}^{n} a_\nu X^\nu.$$

Man får en ring $L := K[Y]/\sim$ som omfattar K och där ekvivalensklassen $\overline{Y} \in L$ uppenbarligen är ett nollställe till f.

Det återstår att kolla om L är en kropp: Det är så omm polynomet f är *irreducibelt*, dvs. inte kan faktoriseras som en produkt $f = gh$ av polynom $g, h \in K[X]$ av mindre grad.

Vi börjar med konstruktionen av faktorringar:

Definition 8.1. Låt R vara en kommutativ ring och $\mathfrak{a} \subset R$ ett ideal.

1. En restklass mod $\mathfrak{a}$ är en mängd

$$x + \mathfrak{a} := \{x + a; a \in \mathfrak{a}\}.$$

2. Mängden

$$R/\mathfrak{a} := \{x + \mathfrak{a}; x \in R\}$$

av alla restklasser mod idealet $\mathfrak{a}$ utrustas med två operationer

(a) additionen

$$R/\mathfrak{a} \times R/\mathfrak{a} \longrightarrow R/\mathfrak{a}$$

$$(x + \mathfrak{a}, y + \mathfrak{a}) \mapsto (x + \mathfrak{a}) + (y + \mathfrak{a}) = (x + y) + \mathfrak{a},$$

som är den elementvisa summan av de två restklasserna $x + \mathfrak{a}$ och $y + \mathfrak{a}$, och

(b) multiplikationen

$$R/\mathfrak{a} \times R/\mathfrak{a} \longrightarrow R/\mathfrak{a}$$

$$(x + \mathfrak{a}, y + \mathfrak{a}) \mapsto (x + \mathfrak{a})(y + \mathfrak{a}) + \mathfrak{a} = xy + \mathfrak{a},$$

som är den "påfyllda" elementvisa produkten av de två restklasserna $x + \mathfrak{a}$ och $y + \mathfrak{a}$,

Example 8.2. För $R = \mathbb{Z}, \mathfrak{a} = (n) := \mathbb{Z}n$ får vi

$$\mathbb{Z}/(n) = \mathbb{Z}_n.$$

Remark 8.3. 1. Restklasserna $x+\mathfrak{a}$ är ekvivalensklasserna till ekvivalensrelationen

$$x \sim y :\Longleftrightarrow y - x \in \mathfrak{a}$$

på R. I synnerhet gäller

$$x + \mathfrak{a} = y + \mathfrak{a} \text{ eller } (x + \mathfrak{a}) \cap (y + \mathfrak{a}) = \emptyset.$$

2. Kvotavbildningen

$$R \longrightarrow R/\mathfrak{a}, x \mapsto x + \mathfrak{a},$$

är en surjektiv ringhomomorfism.

Vi presenterar en explicit beskrivning av faktorringen $L := K[X]/(f)$.

Definition 8.4. Vi definierar $K[X]_{<m} \subset K[X]$ som den delmängd till polynomringen över K, vars element har högst grad $m - 1$., dvs.

$$K[X]_{<m} := \{h \in K[X]; \text{grad}(h) < m\}.$$

Remark 8.5. 1. Avbildningen

$$K^m \longrightarrow K[X]_{<m},$$

$$(\lambda_0, ..., \lambda_{m-1}) \mapsto \lambda_{m-1}X^{m-1} + \lambda_{m-2}X^{m-2} + ... + \lambda_1 X + \lambda_0$$

är en bijektion.

2. Delmängden $K[X]_{<m}$ är additivt sluten, men inte multiplikativt.

Theorem 8.6. *Låt $f \in K[X], m := \text{grad}(f) > 0$ och $\mathfrak{a} := (f)$. Sedan har vi*

1. *$K[X]_{<m} \cap \mathfrak{a} = \{0\}$ och*
2. *$K[X] = K[X]_{<m} + \mathfrak{a}$.*

I synnerhet är sammansättningen

$$K[X]_{<m} \hookrightarrow K[X] \longrightarrow L := K[X]/(f)$$

av inklusionen och kvotavbildningen bijektiv. Med andra ord: Varje element $c \in L$ är en entydig linjärkombination

$$c = \lambda_{m-1}a^{m-1} + \lambda_{m-2}a^{m-2} + ... + \lambda_1 a + \lambda_0$$

av potenserna $1, a, ..., a^{m-1}$ *till restklassen* $a := \overline{X}$ *med koefficienter* $\lambda_0, \lambda_1, ..., \lambda_{m-1} \in K$. *Ytterligare, om*

$$K[X]_{<m} \times K[X]_{<m} \longrightarrow K[X]_{<m},$$

$$(g, h) \mapsto g * h,$$

är avbildningen som motsvarar multiplikationen

$$L \times L \longrightarrow L$$

under denna bijektion, så har vi

$$g * h = r,$$

där $r \in K[X]_{<m}$ *är resten man får vid division av* gh *genom* f, *dvs.*

$$gh = q \cdot f + r.$$

Proof of Th.8.6. Följer omedelbart från Th.7.13, divisionsalgoritmen för polynom. □

Remark 8.7. För räkningar i L kan man använda sig antingen av divisionsalgoritmen eller notera att, om $f = X^m - \sum_{\mu=0}^{m-1} \beta_\mu X^\mu$, så gäller

$$a^m = \sum_{\mu=0}^{m-1} \beta_\mu a^\mu$$

för $a := \overline{X}$.

Example 8.8. Avbildningen $\mathbb{R}[X]/(X^2+1) \longrightarrow \mathbb{C}, \alpha + \beta\overline{X} \mapsto \alpha + \beta i$ är en ringisomorfism.

Det återstår att kolla när L är en kropp:

Theorem 8.9. *För ett polynom* $f \in K[X] \backslash K$ *och* $L := K[X]/(f)$ *är följande påståenden ekvivalenta:*

1. *Ringen* L *är en kropp.*
2. *Ringen* L *är ett integritetsområde.*

3. Polynomet $f \in K[X]$ är irreducibelt.

Proof. "1) $\Longrightarrow$ 2)": Självklart!
"2) $\Longrightarrow$ 3)": Om f är reducibelt (=icke-irreducibelt), dvs. $f = gh$, så har L nolldelare:

$$0 = \overline{g} \cdot \overline{h}.$$

"3) $\Longrightarrow$ 1)": Låt $\overline{g} \in L \setminus \{0\}$. Enligt Prop.7.14 nedan kan vi skriva

$$K[X]g + K[X]f = K[X]h$$

med ett entydigt bestämt normerat polynom $h \in K[X]$. Polynomet h delar det irreducibla polynomet f; således $h = f$ eller $h = 1$. Men h delar också g och $\overline{g} \neq 0$, så nödvändigtvis $g = 1$. Det finns alltså polynom $p, q \in K[X]$ med

$$1 = p \cdot g + q \cdot f$$

resp.

$$1 = \overline{p} \cdot \overline{g}.$$

□

Example 8.10. 1. Om $d \in K$ inte är en kvadrat, så är $X^2 - d \in K[X]$ irreducibelt och

$$L := K[X]/(X^2 - d)$$

är en kropp. Man använder sig ofta av den symboliska notationen

$$\sqrt{d} := \overline{X},$$

eftersom ju $\overline{X}^2 = d \in K \subset L$. Vi har då

$$L = K + K\sqrt{d}.$$

I fall $d = -1$ skriver vi också

$$i := \sqrt{-1},$$

vi får således "komplexa tal med K-koefficienter" $\alpha + \beta i, \alpha, \beta \in K$.

2. Polynomet $X^2 + X + 1 \in \mathbb{Z}_2[X]$ är irreducibelt och

$$\mathbb{F}_4 := \mathbb{Z}_2[X]/(X^2 + X + 1)$$

en kropp med 4 element.

Sammanfattningsvis kan vi konstatera:

Theorem 8.11. *Låt K vara en kropp.*

1. *Om $f \in K[X]$ är ett irreducibelt polynom, så finns det en kroppsutvidgning $L \supset K$ tillsammans med ett element $a \in L$, sådant att $f(a) = 0$.*

2. *För varje polynom $f \in K[X]$ finns det en "rotkropp" E, dvs. en kroppsutvidgning $E \supset K$, sådant att $f \in E[X]$ är en produkt av linjära polynom.*

Proof. 1.) Ta $L := K[Y]/(f(Y)) \supset K, a := \overline{Y}$, där $f(Y)$ uppstår från $f = f(X)$ genom namnbyte av "variabeln".
2.) Induktion följande grad(f). Ta ett irreducibelt polynom $p \in K[X]$ som delar f. Enligt 1) finns $L \supset K$ med $a \in L, p(a) = 0$. Skriv $f = (X - a)g, g \in L[X]$, och använd induktionshypotesen på $g \in L[X]$ för att få $E \supset L$. Utvidgningen $E \supset L \supset K$ är då det vi letar efter. □

Om vi har $K = \mathbb{Q}$, så är ovanstående sats inte särskilt spännande: Pga. algebrans fundamentalsats Th.12.3 kan vi välja $E = \mathbb{C}$ oberoende av polynomet f. Men i vilken relation står då vår formella konstruktion och komplexa talkroppen? Ja, den första är isomorf med en delkropp till $\mathbb{C}$.

Proposition 8.12. *Om $\varphi : R \longrightarrow S$ är en ringhomomorfism och $\mathfrak{a} := \ker(\varphi)$, så är*

$$R/\mathfrak{a} \longrightarrow S, x + \mathfrak{a} \mapsto \varphi(x),$$

en injektiv ringhomomorfism och inducerar en ringisomorfism

$$R/\mathfrak{a} \longrightarrow \varphi(R).$$

I synnerhet, om $b \in E \supset K$ med en kroppsutvidgning $E \supset K$ och $f(b) = 0$ med ett irreducibelt polynom $f \in K[X]$, finns det en injektiv ringhomomorfism

$$L := K[Y]/(f(Y)) \hookrightarrow E, \overline{Y} \mapsto b.$$

Proof. Första delen rekommenderas som övning till läsaren. Utvärderingen $\varepsilon_b : K[Y] \longrightarrow E, g \mapsto g(b)$, har $\ker(\varepsilon_b) = (f(Y))$. I alla fall har vi $\ker(\varepsilon_b) = (h)$ med något polynom $h \in K[Y] \setminus K$ och $h | f(Y)$ pga. $0 = f(b) = \varepsilon_b(f)$. Men $f(Y)$ är irreducibelt, således $h \in K^* f(Y)$ och $(h) = (f(Y))$. □

Definition 8.13. Låt $L \supset K$ vara en kroppsutvidgning.

1. En kroppsutvidgning $L \supset K$ kallas *enkel*, om det finns ett element $a \in L$ sådant att
$$L = K[a] := \varepsilon_a(K[X])$$
med utvärderingshomomorfismen
$$\varepsilon_a : K[X] \longrightarrow L, g \mapsto g(a).$$

2. Om för ett element $a \in L$ utvärderingshomomorfismen $\varepsilon_a : K[X] \longrightarrow L$ inte är injektiv, kallas det entydiga normerade (och irreducibla) polynomet $p_a \in K[X]$ med
$$\ker(\varepsilon_a) = (p_a)$$
minimalpolynomet till $a \in L$ över K.

Remark 8.14. 1. För $f \in K[X]$ har vi
$$f(a) = 0 \Longleftrightarrow p_a | f.$$

2. Om $f(a) = 0$ med det normerade och irreducibla polynomet $f \in K[X]$, så gäller $p_a = f$.

Example 8.15. Låt oss diskutera hur konstruktionen av rotkroppen $E \supset \mathbb{Q}$ fungerar för de irreducibla kubiska polynomen

1. $f = X^3 - 2 \in \mathbb{Q}[X]$,

2. $f = X^3 - 3X + 1 \in \mathbb{Q}[X]$.

Ta $L := \mathbb{Q}[Y]/(f(Y))$. I det första fallet har vi en injektiv ringhomomorfism
$$L \hookrightarrow \mathbb{R}, a := \overline{Y} \mapsto b := \sqrt[3]{2}.$$
Om vi nu skriver
$$f = (X - a)g$$
är andra faktorn $g \in L[X]$ irreducibelt, eftersom
$$L \cong \mathbb{Q}\left[\sqrt[3]{2}\right] \subset \mathbb{R}$$

och de komplexa nollställena till g är de icke-reella talen

$$\sqrt[3]{2}\varepsilon, \sqrt[3]{2}\varepsilon^2$$

med $\varepsilon := \frac{1}{2}(-1+i\sqrt{3})$. I fallet $f = X^3-3X+1$ visar en liten räkning att inte bara $f(a) = 0$, utan också $f(a^2-2) = 0$ och sedan också $f(2-a-a^2) = 0$ pga. $(a^2-2)^2-2 = 2-a-a^2$. Eftersom de här nollställena är parvis olika, är polynomet f redan i $L[X]$ en produkt av linjära polynom, dvs. vi kan välja $E = L$, medan det inte går i det första fallet.

För fullständighetens skull presenterar vi en injektion in i den reella talkroppen också i det andra fallet:

$$L \hookrightarrow \mathbb{R}, a := \overline{Y} \mapsto b := 2\cos\left(\frac{2\pi}{9}\right).$$

Det är väl lättast att kolla att $f(b) = 0$, om man skriver $b = \zeta + \zeta^{-1}$ med $\zeta = \exp\left(\frac{2\pi i}{9}\right)$. De andra två nollstälena till f blir

$$2\cos\left(\frac{4\pi}{9}\right),\ 2\cos\left(\frac{8\pi}{9}\right).$$

I båda fall har vi tre injektioner $L \hookrightarrow \mathbb{C}$ motsvarande de komplexa nollställena till f; i det andra fallet är de alla reella, medan i det första fallet är bara en av dem reell.

9 Primitiva rötter

Hittills har vi sett några exempel på ändliga kroppar $\mathbb{F}$, och så småningom ska vi komma fram till en fullständig klassifikation, se Th. 10.2. Det avgörande är att förstå den multiplikativa strukturen:

Theorem 9.1. *Låt $\mathbb{F}$ vara en ändlig kropp, $q = |\mathbb{F}|$. Sedan finns det en primitiv rot $a \in \mathbb{F}$, dvs. sådant att*

$$\mathbb{F}^* = a^{\mathbb{Z}} = \{1, a, ..., a^{q-2}\}.$$

(Kom ihåg att $a^{q-1} = 1$ enligt Lagranges sats Th.4.13).)

Example 9.2. 1. Restklassen $a = \overline{2} \in \mathbb{Z}_{11}$ är en primitiv rot: Den har potenser

$$\overline{1}, \overline{2}, \overline{4}, \overline{8}, \overline{5}, \overline{10} = -\overline{1}, -\overline{2} = \overline{9}, -\overline{4} = \overline{7}, -\overline{8} = \overline{3}, -\overline{5} = \overline{6}, \overline{1}, \overline{2}, ...$$

Vi får alltså en periodisk följd med minsta perioden 10.

2. Eller ta $a = 5+5i \in \mathbb{Z}_7[i] \cong \mathbb{Z}_7[X]/(X^2+1)$, en kropp med 49 element. Vi får potenserna:

$$1, 5+5i, i, 2+5i, -1, 2+2i, -i, 5+2i, 1, 5+5i, ...$$

en periodisk följd med minsta perioden 8. Så a är inte en primitiv rot för $\mathbb{Z}_7[i]$. Men vi har $a = b^2$ med $b = 3+2i$. Följden $1, b, b^2, ...$ har då minsta perioden 16, så det är inte heller en primitiv rot, men lite närmare ändå.

Remark 9.3. Om $n = \ell(q-1)+r; 0 \leq r < q-1$, så har vi $a^n = a^r$ pga. $a^{q-1} = 1$ (Lagranges sats Th.4.13).

Corollary 9.4. *En ändlig kropp $\mathbb{F}$ är en enkel utvidgning*

$$\mathbb{F} = \mathbb{Z}_p[a] \supset P(\mathbb{F}) = \mathbb{Z}_p$$

av sin primkropp.

Proof. För en primitiv rot a till $\mathbb{F}$ har vi

$$\mathbb{F} = a^{\mathbb{Z}} \cup \{0\} \subset \mathbb{Z}_p[a] \subset \mathbb{F}.$$

□

Corollary 9.5. *Låt p vara ett udda primtal. Sedan är $-1 \in \mathbb{Z}_p$ en kvadrat omm $p = 4k+1$.*

Proof. 1. Anta $p = 4k+1$ och låt $a \in \mathbb{Z}_p^*$ vara en primitiv rot:

$$1 = a^{4k} = (\underbrace{a^{2k}}_{\neq 1})^2 \Longrightarrow (a^k)^2 = a^{2k} = -1,$$

eftersom ekvationen $x^2 = 1$ har i en kropp bara lösningarna ± 1 pga. $x^2 - 1 = (x+1)(x-1)$.

2. Anta $p = 4k+3$ och $j \in \mathbb{Z}_p, j^2 = -1$. Sedan:

$$1 = j^{4k+2} = (j^2)^{2k+1} = (-1)^{2k+1} = -1,$$

motsägelse.

□

Example 9.6. * Vi kan nu för alla udda primtal skapa kroppar $\mathbb{F}$ med p^2 element. Ta en primitiv rot $a \in \mathbb{Z}_p$ och $\mathbb{F} = \mathbb{Z}_p\left[\sqrt{d}\right]$ med $d = a^{2\ell+1}$. Vi lämnar det som övning till läsaren att visa, att det blir isomorfa kroppar, oberoende av talet $\ell \in \mathbb{N}$. Om $p = 4k+3$ och vi tar $\ell = k$, får vi $d = -1$ och $\mathbb{F} = \mathbb{Z}_p[i]$ - komplexa tal med $\mathbb{Z}_p$-koefficienter.

Låt R vara en kommutativ ring. Vi undersöker först potenserna av enstaka element $a \in R^*$ i enhetsgruppen till R.

Definition 9.7. För ett element $a \in R^*$ definieras dess ordning som

$$\mathrm{ord}(a) := \min\{k \in \mathbb{N}_{>0}, a^k = 1\},$$

där vi använder oss av konventionen

$$\min \emptyset := \infty.$$

Example 9.8.

1. Restklassen $a = \overline{2} \in \mathbb{Z}_{11}$ har $\mathrm{ord}(\overline{2}) = 10$.
2. Titta på $5+5i, 3+2i \in \mathbb{Z}_7[i]$, Vi hittar $\mathrm{ord}(5+5i) = 8, \mathrm{ord}(3+2i) = 16$.
3. För ett komplext tal
$$a = re^{i\vartheta} \in \mathbb{C}^*$$
gäller
$$\mathrm{ord}(a) < \infty \Longleftrightarrow r = 1 \wedge \vartheta \in \mathbb{Q} \cdot 2\pi.$$
I själva verket
$$\mathrm{ord}(e^{2\pi i(k/n)}) = n,$$
omm $\mathrm{sgd}(k, n) = 1$.

Remark 9.9. Låt R vara en kommutativ ring och $a \in R^*$ en enhet.

1. $\mathrm{ord}(a) = \infty \Longleftrightarrow$ potenserna $a^k, k \in \mathbb{Z}$, är parvis olika.
2. Anta $\mathrm{ord}(a) = d < \infty$. Sedan $a^k = a^\ell \Longleftrightarrow d|(\ell - k)$ samt
$$a^{\mathbb{Z}} = \{\underbrace{1, a, ..., a^{d-1}}_{\text{parvis olika}}\},$$
i synnerhet $|a^{\mathbb{Z}}| = d$.

3. Om $|R^*| < \infty$, så har vi

   (a) $d := \text{ord}(a) < \infty$ och d delar $|R^*|$ pga. $a^{|R^*|} = 1$. (Lagranges sats Th.4.13)

   (b) $R^* = a^{\mathbb{Z}} \Longleftrightarrow \text{ord}(a) = |R^*|$.

   (c) Om $\mu(R^*)$ är den minsta exponenten $n > 0$, sådant att $x^n = 1$ för alla $x \in R^*$, har vi:

$$\mu(R^*) = \text{mgm}\{\text{ord}(x); x \in R^*\}.$$

   (d) Om $a^\ell = 1$ för alla $a \in R^*$, gäller $\ell \in \mathbb{Z} \cdot \mu(R^*)$.

Proposition 9.10. *1. För en ändlig kropp har vi*

$$\mu(\mathbb{F}^*) = |\mathbb{F}^*|.$$

2. Om $\mu(R^*) = |R^*|$, finns det en primitiv rot för R^*.

Proof. 1. Polynomet $f = X^n - 1$ med $n := \mu(\mathbb{F}^*)$ har hela $\mathbb{F}^*$ som nollställemängd. Eftersom $\mathbb{F}$ är ett integritetsområde får vi $n \geq q - 1$. Men $x^{q-1} = 1, \forall x \in R$, innebär $n|(q-1)$, och så måste $n = q - 1$.

2. Vi sätter ihop ett element $a \in R^*$ med

$$\text{ord}(a) = |R^*| = p_1^{k_1} \cdot ... \cdot p_r^{k_r},$$

primfaktoriseringen. Eftersom $\mu(R^*) = |R^*|$ finns det för varje $i = 1, ..., r$ ett element $c_i \in R^*$ med

ord$(c_i) = s_i p_i^{k_i}$. För $a_i = c_i^{s_i}$ blir det då ord$(a_i) = p_i^{k_i}$. Sedan är

$$a = a_1 \cdot ... \cdot a_r$$

enligt Prop.9.12 ett element av ordning $q - 1$.

□

Example 9.11. * Låt oss titta på situationen för en restklassring $\mathbb{Z}_n$ i stället för $\mathbb{F}$.

1. Enhetsgruppen
$$\mathbb{Z}_8^* = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$$
med sina 4 element uppfyller $\mu(\mathbb{Z}_8^*) = 2$.

2. Låt p, q vara två olika udda primtal. Enhetsgruppen
$$\mathbb{Z}_{pq}^* \cong \mathbb{Z}_p^* \times \mathbb{Z}_q^*$$
har $(p-1)(q-1)$ element. men
$$a^\ell = 1$$
gäller redan för $\ell = (p-1)(q-1)/2$, eftersom ℓ är både delbart med $p-1$ och med $q-1$.

3. Enhetsgruppen $\mathbb{Z}_{p^k}^*$ för ett primtal p har en primitiv rot: Välj $\overline{a} \in \mathbb{Z}_{p^k}^*$, sådant att $a + \mathbb{Z}p$ är en primitiv rot för $\mathbb{Z}_p^*$. Således $\operatorname{ord}(\overline{a}) = p^\ell(p-1)$ med något $\ell \leq k-1$, medan $\operatorname{ord}(\overline{1+p}) = p^{k-1}$. Det följer
$$\mu(\mathbb{Z}_{p^k}^*) = p^{k-1}(p-1) = |\mathbb{Z}_{p^k}^*|.$$

Proposition 9.12. *1. Låt* $\operatorname{ord}(a) = m$*, Sedan gäller*
$$\operatorname{ord}(a^k) = \frac{m}{\operatorname{sgd}(k,m)}.$$

2. Om $m = \operatorname{ord}(a)$ *och* $n = \operatorname{ord}(b)$ *är relativ prim, så gäller*
$$\operatorname{ord}(ab) = mn.$$

Proof. 1. Vi har
$$1 = (a^k)^\ell = a^{k\ell} \iff m | k\ell \iff \frac{m}{\operatorname{sgd}(k,m)} | \ell.$$

2. Låt
$$1 = (ab)^\ell \Longrightarrow a^\ell = b^{-\ell} \Longrightarrow \operatorname{ord}(a^\ell) = \operatorname{ord}(b^{-\ell})$$
$$\Longrightarrow \frac{m}{\operatorname{sgd}(\ell,m)} = \frac{n}{\operatorname{sgd}(\ell,n)},$$
dvs. $1 = 1$ och
$$\operatorname{sgd}(\ell,m) = m, \operatorname{sgd}(\ell,n) = n \Longrightarrow \ell \in \mathbb{Z} \cdot mn.$$

□

10 Ändliga kroppar

Theorem 10.1. *Låt $F \supset \mathbb{Z}_p$ och $L \supset \mathbb{Z}_p$ vara ändliga kroppar. Om $|F| = |L|$, gäller redan $F \cong L$.*

Proof. Låt $q = |F| = |L| = p^m$. Enligt Cor.9.4 har vi

$$F = \mathbb{Z}_p[a]$$

med något $a \in F$. Eftersom $|F| < \infty$, är utvärderingshomomorfismen $\varepsilon_a : \mathbb{Z}_p[X] \longrightarrow F$ inte injektiv och elementet a har således ett minimalpolynom $p_a \in \mathbb{Z}_p[X]$. Eftersom polynomet $X^q - X \in \mathbb{Z}_p[X]$ annullerar hela F, har det enligt Rem.8.14.1 polynomet p_a som delare:

$$p_a \cdot h = X^q - X = \prod_{c \in L}(X - c).$$

Så det finns $b \in L$ med $p_a(b) = 0$. Med Rem.8.14.2 följer $p_a = p_b$. Således får vi en isomorfism

$$F \cong \mathbb{Z}_p[X]/(p_a) \cong \mathbb{Z}_p[b] = L,$$

där inklusionen $\mathbb{Z}_p[b] \subset L$ faktiskt är en likhet pga. $|\mathbb{Z}_p[b]| = q = |L|$. □

Theorem 10.2. *Låt p vara ett primtal och $n \in \mathbb{N}_{>0}$. Sedan finns det en (så när som på isomorfi entydig) ändlig kropp $\mathbb{F}_{p^n}$ med p^n element. I själva verket har vi*

$$\mathbb{F}_{p^n} \cong \mathbb{Z}_p[X]/(f),$$

för varje irreducibelt polynom $f \in \mathbb{Z}_p[X], \operatorname{grad}(f) = n$. Mängden av sådana polynom är icke-tom.

Proof. För entydigheten hänvisar vi till Teorem 10.1. Låt $q := p^n$. Enligt Th.8.11.2 hittar vi en utvidgning $E \supset \mathbb{Z}_p$, där $f = X^q - X \in \mathbb{Z}_p[X]$ är en produkt av linjära polynom. Vi tar nu

$$\mathbb{F}_q := \{x \in E; \sigma^n(x) = x\}$$

med Frobeniusautomorfismen $\sigma : E \longrightarrow E, x \mapsto x^p$. Det handlar om en kropp, eftersom $\sigma^n : E \longrightarrow E, x \mapsto x^q$, är en automorfism den också. Å andra sidan är $\mathbb{F}_q$ nollställemängden till f. Men f har bara enkla nollställen enligt Ex.7.10 och således $|\mathbb{F}_q| = q$. Slutligen är $\mathbb{F}_q = \mathbb{Z}_p[a]$ en enkel utvidgning och $p_a \in \mathbb{Z}_p[X]$ ett irreducibelt polynom av grad n. □

Example 10.3. 1. Låt $p > 2$ och $d \in \mathbb{Z}_p$ vara en primitiv rot. Sedan är d en icke-kvadrat: Om $d = b^2$ med $b \in \mathbb{Z}_p$, följer ju

$$\overline{1} \neq d^{(p-1)/2} = b^{p-1} = \overline{1}.$$

Således är $X^2 - d \in \mathbb{Z}_p[X]$ irreducibelt och

$$\mathbb{F}_{p^2} := \mathbb{Z}_p\left[\sqrt{d}\right] = \mathbb{Z}_p + \mathbb{Z}_p\sqrt{d}.$$

en kropp med p^2 element.

2. Om $p = 4k + 1$, är $d = -1$ inte en kvadrat och

$$\mathbb{F}_{p^2} \cong \mathbb{Z}_p\left[i\right] = \mathbb{Z}_p + \mathbb{Z}_p i.$$

3. Polynomet $f = X^3 - X - 1 \in \mathbb{Z}_3[X]$ är irreducibelt och

$$\mathbb{F}_{27} = \mathbb{Z}_3/(X^3 - X - 1) = \mathbb{Z}_3 + \mathbb{Z}_3\overline{X} + \mathbb{Z}_3\overline{X}^2$$

en kropp med 27 element.

Remark 10.4. * För nyfikna en liten utblick på Galoisteorin: I beviset av Th.10.1 har vi sett att isomorfismen $F \xrightarrow{\cong} L$ inte är entydig; i själva verket finns det n stycken!

Givet ett polynom $f \in K[X]$, finns det enligt Th.8.11.2 en kroppsutvidgning $E \supset K$, en sammansättning av ändligt många enkla utvidgningar, sådant att $f \in K[X]$ blir en produkt av linjära polynom i $E[X]$. Den (så när som på isomorfi entydiga) minimala sådana utvidgningen $E \supset K$ kallas *rotkroppen* till f. Det man undersöker är denna utvidgningens automorfismer, dvs. ringautomorfismer $\sigma : E \longrightarrow E$, som gör övre delen till diagrammet

$$\begin{array}{ccc} K & \xrightarrow{\mathrm{id}} & K \\ \cap & & \cap \\ E & \xrightarrow{\sigma} & E \\ \cup & & \cup \\ N(f) & \xrightarrow{\sigma} & N(f) \end{array} .$$

kommutativ. Automorfismerna kan sammansättas och inverteras - de utgör utvidgningens *Galoisgrupp* $\mathrm{Aut}_K(E)$. T.ex. har vi

$$\mathrm{Aut}_{\mathbb{Z}_p}(\mathbb{F}_{p^n}) = \varphi^{\mathbb{Z}} = \{\mathrm{id}, \varphi, ..., \varphi^{n-1}\}$$

med Frobeniusautomorfismen $\varphi : \mathbb{F}_{p^n} \longrightarrow \mathbb{F}_{p^n}$.

För $x \in E$ har vi $f(\sigma(x)) = \sigma(f(x))$, eftersom $f \in K[X]$; i synnerhet gäller

$$\sigma(N(f)) = N(f)$$

för nollställemängden

$$N(f) := \{a \in E; f(a) = 0\}.$$

Ifall polynomet f bara har enkla nollställen, kan vi faktiskt identifiera automorfismer till utvidgningen $E \supset K$ med deras restriktion på $N(f) \subset L$ – och på det här sättet var det Galois själv har formulerat sin teori: Vid den tiden fanns inte än ringar, homomorfismer och liknande saker.

I själva verket är $E \supset K$ ofta själv en enkel utvidgning, t.ex. är det alltid så, om $\mathrm{char}(K) = 0$ eller $K = \mathbb{F}$ är en ändlig kropp, men för beräkningar spelar det inte någon stor roll.

11 Gaußiska heltal

Vi har hittills sett två viktiga ringar, där det finns för icke-enheterna ett slags entydig primfaktorisering, heltalsringen $\mathbb{Z}$ och polynomringen $K[X]$ över en kropp K. Här studerar vi ett tredje exempel:

Definition 11.1. Ringen

$$\mathbb{Z}[i] := \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C}$$

av alla Gaußiska heltal är gittret av alla komplexa tal, vars real- och imaginärdel är heltal.

Proposition 11.2. *Enhetsgruppen till ringen av alla Gaußiska heltal är*

$$\mathbb{Z}[i]^* = \{z \in \mathbb{Z}[i]; |z| = 1\} = \{\pm 1, \pm i\}.$$

Proof. Gaußiska heltal $z \in \mathbb{Z}[i] \setminus \{0\}$ uppfyller $|z| \geq 1$; således gäller $z^{-1} \in \mathbb{Z}[i]$ bara om $|z| = 1$, och då får vi $\pm 1, \pm i$ som enheter. □

Proposition 11.3. *Ringen $\mathbb{Z}[i]$ av alla Gaußiska heltal är ett principalidealområde.*

Proof. Låt $\mathfrak{a} \neq \{0\}$ vara ett nollskilt ideal. Ta $d \in \mathfrak{a} \setminus \{0\}$ av minimal längd. Uppenbarligen gäller $\mathbb{Z}[i]d \subset \mathfrak{a}$. Å andra sidan givet ett element $u \in \mathfrak{a}$, approximera det komplexa talet $ud^{-1} \in \mathbb{C}$ genom ett Gaußiskt heltal $b \in \mathbb{Z}[i]$, sådant att

$$|ud^{-1} - b| < 1.$$

Detta är möjligt, eftersom varje komplext tal ligger i en enhetskvadrat vars hörn är gitterpunkter. Avståndet av en punkt i kvadraten till närmaste hörn är högst $1/\sqrt{2} < 1$. I symmerhet

$$|u - bd| < |d|.$$

Eftersom $u - bd \in \mathfrak{a}$, får vi $u - bd = 0$ resp. $u = bd$. □

I det här avsnittet etablerar vi ett slags primtalsfaktorisering för Gaußiska heltal. Men innan vi gör det, låt oss införa tre nya begrepp:

Definition 11.4. Låt R vara ett integritetsområde.

1. Två icke enheter $u, v \in R$ kallas *associerade* om $v = eu$ med en enhet $e \in R^*$.

2. En icke-enhet $u \in R \setminus \{0\}$ kallas *irreducibelt* om den inte kan skrivas som produkt av två icke-enheter.

3. Ett integritetsområde kallas *faktoriellt* om varje icke-enhet $a \in R \setminus \{0\}$ kan skrivas

   $$a = u_1 \cdot \ldots \cdot u_r$$

   som produkt av irreducibla element, där faktorerna är entydiga så när som på omkastning och multiplikation med enheter.

Remark 11.5.

1. Ett Gaußisk heltal z är irreducibelt omm $|z| > 1$ och

   $$z = uv \Longrightarrow |u| = 1 \vee |v| = 1$$

   gäller för $u, v \in \mathbb{Z}[i]$.

2. Om $|z|^2 = p \in \mathbb{N}$ är ett primtal, är $z \in \mathbb{Z}[i]$ irreducibelt, t.ex. $1+i, 1-i, 2+i, 2-i$ är irreducibla Gaußiska heltal.

3. Ett primtal $p \in \mathbb{N}$ behöver inte vara ett irreducibelt Gaußiskt heltal, t.ex.

   $$2 = (1+i)(1-i), 5 = (2+i)(2-i).$$

Theorem 11.6. *$\mathbb{Z}[i]$ är faktoriell.*

Proof. Eftersom $\mathbb{Z}[i]$ är ett principalidealområde, uppfyller irreducibla Gaußiska heltal $u \in \mathbb{Z}[i]$ följande implikation

$$u|ab \Longrightarrow u|a \vee u|b.$$

Detta ger faktoriseringens entydighet, i fall den finns. Men successivt förfinade faktoriseringar tar slut någon gång pga.

$$z = ab, a, b \notin \mathbb{Z}[i]^* \Longrightarrow \mathbb{N} \ni |z|^2 > |a|^2, |b|^2 \in \mathbb{N}.$$

□

Remark 11.7. Varje Gaußiskt heltal är associerat till ett tal $z = x + iy$ i sektorn $0 < |y| \leq x$.

Theorem 11.8. **Faktorisering av primtal $p \in \mathbb{N}$ i ringen $\mathbb{Z}[i]$:**

p	2	$= 4k+3$	$= 4k+1$
	$-i(1+i)^2$	p	$(a+bi)(a-bi); 0 < b < a$

Heltalen a, b är entydiga, $a + bi, a - bi$ är icke-associerade irreducibla Gaußiskt heltal.

Proof. 1. Anta $p = 4k+3 = zw, |z|, |w| > 1$. Det innebär $p = |z|^2 = |w|^2$. Sedan $p = x^2 + y^2, z = x + iy, w = x - iy$. Vi tittar på restklasserma

$$\alpha := \overline{x}, \beta := \overline{y} \in \mathbb{Z}_p^*.$$

De uppfyller $\alpha^2 + \beta^2 = 0$ resp. $\gamma^2 = -1$ holds for $\gamma := \alpha\beta^{-1}$. Således $p \equiv 1 \mod (4)$ enligt Cor.9.5.

2. Vi vet att det finns en restklass $j \in \mathbb{Z}_p$ with $j^2 = -\overline{1}$ och tittar på ring homomorfismen

$$\psi : \mathbb{Z}[i] \longrightarrow \mathbb{Z}_p, x + yi \mapsto \overline{x} + \overline{y}j.$$

Dess kärna uppfyller

$$\ker(\psi) := \{u \in \mathbb{Z}[i]; \psi(u) = 0\} \supsetneq \mathbb{Z}[i]p;$$

inklusionen är äkta, eftersom annars vore

$$\psi|_Q : Q \hookrightarrow \mathbb{Z}_p$$

med

$$Q := \{x + yi \in \mathbb{Z}[i], 0 \leq x, y < p\}$$

injektiv. Å andra sidan

$$\ker(\psi) = \mathbb{Z}[i]z$$

med ett Gaußsikt heltal z. I synnerhet

$$p = zw.$$

och $p^2 = |z|^2 \cdot |w|^2$. Eftersom $(p) \subsetneqq (z) \subsetneqq \mathbb{Z}[i]$, har vi $z, w \notin \mathbb{Z}[i]^*$, och därför

$$|z|^2 = p = |w|^2, w = \overline{z}.$$

Entydighet har vi pga. aritmetikens fundamentalsats för $\mathbb{Z}[i]$.

□

Remark 11.9. Några praktiska tips för Gaußisk primfaktorisering: Låt $z = x + iy \in \mathbb{Z}[i]$.

1. Skriv

$$z = \text{sgd}(x, y)z_0,$$

faktorisera $\text{sgd}(x, y) \in \mathbb{N}$ på det vanliga sättet och efteråt dela upp primdelarna $p \equiv 1 \mod (4)$ som $p = (a+bi)(a-bi)$ och $2 = -i(1+i)^2$.

2. F.o.m. nu ska vi anta $\text{sgd}(x, y) = 1$. I så fall vet vi

$$z\overline{z} = |z|^2 = 2^k \prod_{\nu=1}^{r} p_\nu^{k_\nu}$$

med primtal $p_\nu \equiv 1 \mod (4), p_1 < p_2 ... < p_r$. Det följer pga. $\text{sgd}(x, y) = 1$ att

$$z = e(1 + i)^k \prod_{\nu=1}^{r} (a_\nu \pm ib_\nu)^{k_\nu},$$

där $e \in \{\pm 1, \pm i\}$ och tecknet beror bara på indexet ν.

3. Skriv
$$w = (1+i)^{-k}z = \frac{1}{2^k}(1-i)^k z.$$

4. För att bestämma tecknet fötr $\nu = 1$, kolla delbarhet med p_1, dvs.: Om
$$p_1 | w \cdot (a_1 \mp b_1 i),$$
så är det $a_1 \pm ib_1$ som gäller.

5. Låt, med rätt tecken,
$$w_1 := \frac{w \cdot (a_1 \mp b_1 i)^{k_1}}{p_1^{k_1}} = e \prod_{\nu=2}^{r} (a_\nu \pm i b_\nu)^{k_\nu}$$
och fortsätt!

Example 11.10. Vi primfaktoriserar $z = 201+43i \in \mathbb{Z}[i]$. Vi har $\mathrm{sgd}(201, 43) = 1$ och
$$z\overline{z} = |z|^2 = 42250 = 2 \cdot 5^3 \cdot 13^2.$$
Således
$$z = e \cdot (1+i)(2 \pm i)^3 (3 \pm 2i)^2 = (1+i)w$$
med
$$w = \frac{1}{2}(1-i)(201+43i) = 122 - 79i.$$
Nu är
$$(2-i)(122-79i) = 165 - 280i$$
delbart genom 5 och således
$$w = (2+i)(33-56i) = (2+i)^2(2-29i) = -(2+i)^3(5+12i)$$
$$= -(2+i)^3(3+2i)^2.$$
Således
$$z = -(1+i)(2+i)^3(3+2i)^2.$$

Theorem 11.11. *Principalidealområden är faktoriella.*

Remark 11.12. * I stället för ett bevis ger vi bara några kommentarer. Som tidigare bevisar man att för ett irreducibelt element i ett principalidealområde R gäller

$$u|ab \Longrightarrow u|a \wedge u|b.$$

Det kvarstår att visa existensen av en faktorisering för varje icke-enhet. Ett reducibelt element kan faktoriseras som produkt av två icke-enheter. Om de är irreducibla är saken klar, om inte fortsätter man. Men varför kan man inte fortsätta med faktorisering i all oändlighet?

I fall det handlar om $\mathbb{Z}, \mathbb{Z}[i]$ eller $K[X]$ går det naturligtvis inte, eftersom faktorerna i en icke-trivial faktorisering har absolutbelopp/grad mindre än vad produkten har.

Om man nu misslyckas med faktorisering kommer man fram till en följd $(a_n) \subset R$, sådant att a_{n+1} är en äkta delare till a_n (dvs. a_{n+1} skiljer sig inte bara om en enhet från a_n) för alla $n \in \mathbb{N}$. Vi får en växande följd av ideal

$$Ra_1 \subsetneqq Ra_2 \subsetneqq .....$$

Unionen är då också ett (principal)ideal:

$$\bigcup_{n=1}^{\infty} Ra_n = Ra.$$

Men sedan har vi $a \in Ra_n$ för något $n \in \mathbb{N}$ och således

$$Ra_n = Ra = Ra_m, \forall m \geq n.$$

Motsägelse!

Vi anmärker att det finns integritetsområden, där faktoriseringsprocessen inte alltid tar slut, ja, t.o.m. sådant att alla icke-enheter är reducibla!

12 Från naturliga tal till komplexa tal*

"Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk."

Det välkända citatet härstammar från den tyske matematikern Leopold Kronecker. Men vad har människorna egentligen gjort? Hade historien varit systematisk, kunde det ha varit så här:

Man började göra skulder och skrev sina tillgångar och skulder som talpar $(n, s) \in \mathbb{N}^2$ och använde sig av en "additiv lokalisering" för att kunna räkna med dem: På mängden $\mathbb{N}^2$ definierar man en ekvivalensrelation

$$(m, r) \sim (n, s) :\Longleftrightarrow m + s = n + r.$$

Den är kompatibel med den komponentvisa additionen och följande multiplikation

$$(m, r) \cdot (n, s) := (mn + rs, ms + rn),$$

så den inducerar en addition och en multiplikation på mängden av dess ekvivalensklasser

$$\mathbb{Z} := \mathbb{N}/\sim .$$

I själva verket kan den uppfattas som en utvidgning

$$\mathbb{Z} \supset \mathbb{N}$$

genom att identifiera $n \in \mathbb{N}$ med ekvivalensklassen till $(n, 0) \in \mathbb{N}^2$.

Sedan upptäckte man, att ibland kunde det vara bra med lite socialt tänkande och började dela och kom fram till rationella tal

$$\mathbb{Q} := Q(\mathbb{Z}) \supset \mathbb{Z}.$$

Till sist var de gamla grekerna inte längre nöjda med bara rationella tal, eftersom diagonalen till en kvadrat av sidolängd 1 inte riktigt gick att tolka som ett rationellt tal. Som ofta i matematiken för att lösa ett problem, varför inte helt enkelt hitta på det man saknar? Dvs. i det här fallet skulle det bli nya "geometriska tal": Man kan ju tänka sig de rationella talen som vissa punkter på en horisontell linje efter att ha bestämt sig för var $0, 1 \in \mathbb{Q}$ skulle ligga. "Reella tal" skulle sedan motsvara precis punkterna på denna linje och så kommer vi fram till en tredje utvidgning

$$\mathbb{R} \supset \mathbb{Q}.$$

Men en obehaglig känsla blir man inte av med: Vad är en punkt på en linje över huvud taget? Man behöver en formell definition motsvarande geometriska intuitionen. Följande iakttagelse ligger till grund för den:

Varje punkt $x \in \mathbb{R}$ kan tillordnas delmängden

$$\mathbb{Q}_{<x} := \{y \in \mathbb{Q}; y < x\}$$

av alla rationella tal vänster om den, och om vi nu lyckas karakterisera dessa delmängder på ett "intrinsiskt" sätt (dvs. utan att använda reella tal som inte än finns), kan vi helt enkelt ta dem som reella tal.

Definition 12.1. Ett reellt tal är en icke-tom delmängd

$$\alpha \subsetneq \mathbb{Q},$$

som är

1. fullständig nedåt: $y \leq x \in \alpha \Longrightarrow y \in \alpha$,
2. och öppen uppåt: $\forall x \in \alpha \; \exists y \in \alpha : y > x$.

Vi betecknar

$$\mathbb{R} \subset \mathcal{P}(\mathbb{Q})$$

mängden av alla dessa reella tal.

Remark 12.2.
1. Ett par (A, B), där A är ett reellt tal i ovanstående bemärkelse och $B := \mathbb{Q} \setminus A$ kallas också ett *Dedekindsnitt*.
2. Rationella tal är reella tal: Vi har en injektiv avbildning

$$\mathbb{Q} \hookrightarrow \mathbb{R}, x \mapsto \mathbb{Q}_{<x}.$$

Naturligtvis är Def.12.1 ingenting för praktiska ändamål, utan dess mening är att ha en modell som uppfyller alla krav man förväntar sig. Efteråt använder man sig bara av egenskaperna våra reella tal har, inte deras explicita form.
Ordningsrelationen definieras som inklusion:

$$\alpha \leq \beta :\Longleftrightarrow \alpha \subset \beta.$$

Aritmetiska operationer för reella tal: Summan av två reella tal är elementvis

$$\alpha + \beta = \{x + y; x \in \alpha, y \in \beta\},$$

medan mulitiplikationen definieras först för positiva rella tal:

$$\alpha \cdot \beta := \alpha^+ \beta^+ \cup \mathbb{Q}_{\leq 0}$$

med den elementvisa produkten

$$\alpha^+ \beta^+ = \{xy; x \in \alpha^+, y \in \beta^+\}$$

av mängderna $\alpha^+ = \alpha \cap \mathbb{Q}_{>0}, \beta^+ = \beta \cap \mathbb{Q}_{>0}$. Till sist utvidgar man multiplikationen

$$\mathbb{R}_{>0} \times \mathbb{R}_{>0} \longrightarrow \mathbb{R}$$

till alla reella tal

$$\mathbb{R} \times \mathbb{R} \longrightarrow \mathbb{R}$$

på det sedvanliga sättet.
Fullständighet: Lägsta övre gränsen (supremum) till en icke-tom begränsad mängd $M \subset \mathbb{R}$ är

$$\sup M := \bigcup_{\alpha \in M} \alpha.$$

Så det blev ganska enkelt! Om man däremot hade försökt definiera allt det där med hjälp av decimalutvecklingen, hade det blivit en massa krångel, inte minst pga. icke-entydigheten fast den ju egentligen verkar förhållandevis harmlös.

Problemet med längden av en kvadrats diagonal är nu löst: Fullständigheten ger existensen av kvadratrötter för $x \in \mathbb{R}_{\geq 0}$, nämligen:

$$\sqrt{x} := \sup\{y \in \mathbb{R}; y^2 \leq x\}.$$

Men negativa tal orsakar fortfarande problem. Så uppfanns det för bekvämlighetens skull imaginära enheten i som ett "symboliskt tal som uppfyller $i^2 = -1$" samt komplexa tal som kombinationer av reella tal med imaginära enheten:

$$\mathbb{R} + \mathbb{R}i = \mathbb{C} \supset \mathbb{R}.$$

I modernt språk använde man sig alltså av definitionen

$$\mathbb{C} := \mathbb{R}[X]/(X^2 + 1)$$

med $i := \overline{X}$ utan att veta det. En liten elementär räkning visar nu att varje komplext tal har en kvadratrot, dvs. man är inte längre tvungen att "skapa" allt fler kvadratrötter. Och om man kommer på idén att använda sig av polärkoordinater, så ser man att det även finns n-te rötter till ett givet komplext tal

$$z = r(\cos(\varphi) + i \sin(\varphi)),$$

nämligen talen

$$w_\nu := \sqrt[n]{r}(\cos\left(\frac{1}{n}(\varphi + 2\pi\nu)\right) + i \sin\left(\frac{1}{n}(\varphi + 2\pi\nu)\right), \nu = 0, ..., n-1.$$

Men situationen är ännu bättre än så:

Theorem 12.3 (**Algebrans fundamentalsats**). *Varje icke-konstant polynom $f \in \mathbb{C}[X]$ har ett komplext nollställe.*

Bevis: Beviset är ett existensbevis, det är inte konstruktivt. Det görs i två steg:

1. Funktionen $f : \mathbb{C} \longrightarrow \mathbb{C}$ har ett minimalställe $z_0 \in \mathbb{C}$, dvs. sådant att

   $$|f(z)| \geq |f(z_0)|$$

   gäller för alla $z \in \mathbb{C}$.

2. Minimalställen för en polynomfunktion är redan nollställen. I själva verket visar man motsatsen: En punkt $z_0 \in \mathbb{C}$ med $f(z_0) \neq 0$ är aldrig ett minimalställe för f: Nära till z_0 finns alltid punkter z med

   $$|f(z)| < |f(z_0)|.$$

   Detta är uppenbarligen fel för kroppen $\mathbb{R}$ i stället för $\mathbb{C}$; den avgörande egenskapen av $\mathbb{C}$ är att för varje $n \in \mathbb{N}$ och $z \in \mathbb{C}$ finns det en n-te rot i $\mathbb{C}$.

1.) **Existens av minimalställen:** Välj en följd $(z_\mu)_{\mu\in\mathbb{N}} \subset \mathbb{C}$ av komplexa tal med

$$\lim_{\mu\to\infty} |f(z_\mu)| = \inf\{|f(z)|; z \in \mathbb{C}\}.$$

Vi visar att följden har en hopningspunkt z_0 – det eftertraktade minimalstället. Vi får anta att polynomet f är normerat, dvs.

$$f(z) = z^n + \sum_{\nu=0}^{n-1} a_\nu z^\nu.$$

För $|z| \gg 0$ är z^n den dominerande termen: Skriv

$$f(z) = z^n \left(1 + \sum_{\nu=0}^{n-1} \frac{a_\nu}{z^{n-\nu}}\right) = z^n K(z).$$

Klammeruttrycket $K(z)$ uppfyller

$$\lim_{z\to\infty} K(z) = 1,$$

eftersom varje term i summan går mot 0 för $z \to \infty$. Således

$$\lim_{z\to\infty} f(z) = \lim_{z\to\infty} z^n = \infty.$$

Men det innebär att följden $(z_\mu)_{\mu\in\mathbb{N}}$ är begränsad, och begränsade följder, säger Bolzano och Weierstraß, har alltid hopningspunkter.

2.) **Ett icke-nollställe z_0 är aldrig ett minimalställe**: Vi får anta $z_0 = 0$ - om inte det är fallet ersätt $f(z)$ med $f(z + z_0)$. Vi skriver

$$f(z) = a_0 + a_m z^m + z^{m+1} g(z)$$

med $a_0, a_m \neq 0$ och

$$g(z) = a_n z^{n-m-1} + \sum_{\nu=m+1}^{n-1} a_\nu z^{\nu-m-1}$$

för $n > m$, medan

$$g(z) \equiv 0$$

för $n = m$. Ta $b \in \mathbb{C}$ med

$$b^m = -\frac{a_0}{a_m}.$$

och undersök funktionen $f(z)$ på halvstrålen

$$\mathbb{R}_{\geq 0} \cdot b = \{tb, t \geq 0\}.$$

Det blir så här:

$$f(tb) = a_0(1 - t^m + t^{m+1} h(t))$$

med

$$h(t) := \frac{b^{m+1}}{a_0} g(tb).$$

Eftersom ju $f(0) = a_0 \neq 0$, räcker det att visa

$$|1 - t^m + t^{m+1} h(t)| < 1$$

för tillräckligt litet $t > 0$. Med

$$M := \max_{0 \le t \le 1} |h(t)|$$

och triangelolikheten får vi uppskattningen:

$$|1 - t^m + t^{m+1}h(t)| \le |1 - t^m| + t^{m+1}M$$

$$= 1 - t^m + t^{m+1}M = 1 - t^m(1 - tM) < 1,$$

om $0 < t < \min(1, \frac{1}{M})$. Ty för $0 \le t \le 1$ har vi ju $|1 - t^m| = 1 - t^m$ och för $t < \frac{1}{M}$ blir det $1 - tM > 0$. □

Kroppar som uppfyller algebrans fundamentalsats får ett eget adjektiv:

Definition 12.4. En kropp K kallas *algebraiskt sluten* om varje polynom $f \in K[X]$ har ett nollställe $a \in K$.

Proposition 12.5. *Om K är algebraiskt sluten, kan varje polynom $f \in K[X] \setminus K$ faktoriseras som produkt av linjära polynom:*

$$f = \lambda \prod_{\nu=1}^{n} (X - b_\nu)$$

med $\lambda, b_1, ..., b_n \in K$.

Proof. Induktion följande $n = \deg(f)$. För $n = 1$ är saken klar. Om $n > 1$ tar vi fram ett nollställe $a \in K$, faktoriserar $f = (X - a)g$ och använder induktionshypotesen på polynomet g. □